Chapter 1

INTRODUCTION

In RSA algorithm, the encryption is done utilizing the receivers public key. Since a users public key is available to everyone in the network. RSA provides confidentiality but the dominant disadvantage of RSA is that there is no authentication i.e anyone can send messages to anyone.

In existing work RSA algorithm is utilized with RGB model for providing confidentiality and authentication but with less accuracy. Due to less accuracy existing system isn't totally secured.

In proposed work AES encryption technique with RGB color is use to extend the accuracy of the system. It'll provides confidentiality, authentication and greater privacy to the data which is sent across the network.

- **Requirements Of Data Security With Colors Using Rsa**

1. **Eligibility :** -Share the more confidential information
2. **Uniqueness :** - More secure algorithm.
3. **Privacy :** Encryption of result.

a) Data Security With Colors Using Rsa

Technology:

We use RGB color model to provide authentication for both sender andreceiver. The process of converting plain text to cipher text is known as encryption. It is also known as enciphering. Any algorithm which encrypts the data is known as encryption algorithm. The sender uses the encryption algorithm. Encryption process is done using the public key of the receiver. the cipher text is obtained by: **$c \equiv m^e \pmod n$),** where m is the message and (e,n) is the public key.
Restoring the plain text from the cipher text is known as deciphering or decryption. Any algorithm which decrypts the data is known as decryption algorithm. The receiver uses the decryption algorithm. The original message can be obtained using the cipher text as: **$m \equiv c^d \pmod n$**, where c is the cipher text and (d,n) is the private key.

Authentication*:-*

services provide assurance of a participating host identity. Therefore, the availability and distribution of keys should be restricted to only authorize group members according to the policy of trust established for the session. Authentication mechanisms can identify the source of the key material and provide a means to counter various masquerades and replay attacks that may be launched against a secure data transmission.

Integrity *:-*

requires the data and control packets originated at an authorized source not to be intercepted or altered while traversing through the network. The possibility of preventing a denial-of-service attack through the transmission of such packets can be minimized or eliminated.

Confidentiality *:-*

services are essential in creating a private data transmission session. It should also be applied to key management transactions during the exchange of key material and can be applied to session announcements allowing them to advertise publicly through standard methods while keeping the details of the session private.

Authorization *:-*

can be implied to only those entities with specific permission that may use the network to send messages after they have been suitably authenticated.

This paper is organized as follows: Section II presents implementation of RSA algorithm, RGB model. Section III describes how RSA and RGB are integrated. Finally, Section IV concludes the paper.

CHAPTER 2

PROBLEM DEFINITION

2.1 Introduction to Data Security With Colors Using Rsa:

There are many encryption algorithms available and used in information security. These algorithms can be categorized into Symmetric and Asymmetric key encryption. In Symmetric key encryption, only one key is used to encrypt and decrypt data while in Asymmetric keys, two keys are used; private and public keys. The public key is used for encryption and private key is used for decryption for example, RSA. There are examples of symmetric cryptographic algorithms like AES and DES. AES uses various 128,192,256 bit keys while DES uses one 64-bits key. All these algorithms can provide authentication, integrity, confidentiality and authorization to data travel from one point another point.

Authentication services provides the assurance of a participating host identity. Therefore, the availability and distribution of keys should be restricted to only authorize group members according to the policy of trust established for the session. Authentication mechanisms can identify the source of the key material and provide a means to counter various masquerades and replay attacks that may be launched against a secure data transmission.

Integrity requires the data and control packets originated at an authorized source not to be intercepted or altered while traversing through the network. The possibility of preventing a denial-of service attack through the transmission of such packets can be minimized or eliminated.

Confidential services are essential in creating a private data transmission session. It should also be applied to key management transactions during the exchange of key material and can be applied to session announcements allowing them to advertise publicly through standard methods while keeping the details of the session private.

Authorization can be implied to only those entities with specific permission that may use the network to send messages after they have been suitably authenticated.

2.2 Limitations of Data Security With Colors Using Rsa:-

- Key is required for encryption and decryptions.
- Network connectivity must be required.

2.3 Proposed System:

- Proposed system deals with providing security to data with colors and AES encryption technique. This security is in the form of confidentiality and authentication. When providing security to the data simultaneously comparison of the AES algorithm with other encryption algorithm also take place.
- Encryption is a technology which protects sensitive data. Combination of Public and Private Key encryption is used to hide the confidential data of users, and cipher text retrieval[4].

2.4 Highlights :

- Save Manual work.
- Maintain the confidently.
- Secure communications.

.

CHAPTER-3

REQUIREMENT ANALYSIS

3.1 Hardware Requirements:-

- Computer.
- LAN,Switch.

3.2 Software Requirements:-

- Language used: Java netbeans.
- Database used : MySql
- Platform: windows 7/8/10:32-bit ,64-bit
- RAM: Minimum 1Gb to Maximum

Chapter 4
FEASIBILITY STUDY

4.1 Cost Estimation

The cost estimation of a software project depends on the following factors

1. Man-Hours.

2. Material.

3. Machines.

4. Software resources involved.

The overheads involve

1. The establishment charges.

2. Depreciation of tools and plants.

3. Licenses of technologies involved in development of software product.

4.1.1 Man-Hours

Man hours state a software project in terms of time required for development. The scope of this project is medium hence cost of time is medium, the man hours required after calculation is around 180 working hours. The back-end required 25 hours of coding and planning and designing of business logic required 30 hours..
.

The front-end coding required 30 hours and planning and designing of pages required 40 hours of man- hours. Another 25 hours were required for testing. As some bugs were detected after the testing phase the corrective action also required time. The debugging process required another 30 hours.

4.1.2 Material:

The material here refers to the electronic devices and networking components that are involved in the practical implementation of the system. Certain costs are incurred due to the use of intranet in the system. The system comprises multiple computers connected in network. So, CAT 6 LAN cables are used to connect the

computers. Further a networking switch is involved in the network topology. Printer is needed to print the report if needed by the higher authority. The system uses internet for generation of reports in the graphical format. So, further a modem of a USB dongle will be required for internet access. The cost of internet access should be also taken into consideration.

4.1.3 Machines:

Machines here include the server and the client computers where the application software is being used. The server needs to be of high specification and with good performance, hence the cost of server is high. The number of computers in the Intranet will decide the cost of client machines.

4.1.4 Software Resources:

The software resource used in the development of a project adds some costs in the overall development process. The licenses of software tool are needed to be purchased for legally using those technologies. In this project all the software and technologies used are licensed under the GNU General Public License (GPL) and are free to use. Technologies like c# is an open source technology which is freely available for use. The database management software used is "MySQL database" which is also open source and is registered under GNU license

4.2 FEASIBILITY STUDY

Introduction

Feasibility study is a test of system proposal according to the workability, impact on the organization, ability to meet user needs and effective use of the available resources. The objective of feasibility study is not to solve the problem but to acquire a sense of its scope.

4.2.1 Technical Feasibility

Evaluating the technical feasibility is the trickiest part of a feasibility study. This is because, at this point in time, not too many detailed design of the system, making it difficult to access issues like performance, costs on (on account of the kind of technology to be deployed) etc. A number of issues have to be considered while doing a technical analysis. Understand the different technologies involved in the proposed system before commencing the project we have to be very clear about what are the technologies that are to be required for the development of the new system. Find out whether the organization currently possesses the required technologies. Technical feasibility centers on the existing system and to what extent it can support the proposed system. The benefits such as high accuracy, minimum response time and user friendliness of the proposed system over weights cost for designing and implementing the new system.

4.2.2 Operational Feasibility

- Proposed project is beneficial only if it can be turned into information systems that will meet the organizations operating requirements. Simply stated, this test of feasibility asks if the system will work when it is developed and installed. Are there major barriers to Implementation? Here are questions that will help test the operational feasibility of a project:
- Is there sufficient support for the project from management from users? If the current system is well liked and used to the extent that persons will not be able to see reasons for change, there may be resistance.
- Are the current business methods acceptable to the user? If they are not, Users may welcome a change that will bring about a more operational and useful systems.
- Have the user been involved in the planning and development of the project?
- Early involvement reduces the chances of resistance to the system and in general and increases the likelihood of successful project.

Since the proposed system was to help reduce the hardships encountered. In the existing manual system, the new system was considered to be operational feasible.

4.2.3 Economics Feasibility

Economic analysis is the most frequently used method for evaluating the effectiveness of a client system. More commonly known as cost/benefit analysis, the procedure is to determine the benefits and savings that are expecting from a client system and compare them with cost.

Economic feasibility attempts to weigh the costs of developing and implementing a new system, against the benefits that would accrue from having the new system in place. This feasibility study gives the top management the economic justification for the new system. A simple economic analysis which gives the actual comparison of costs and benefits are much more meaningful in this case. In addition, this proves to be a useful point of reference to compare actual costs as the project progresses. There could be various types of intangible benefits on account of automation. These could include increased customer satisfaction, improvement in product quality better decision making timeliness of information, expediting activities, improved accuracy of operations, better documentation and record keeping, faster retrieval of information, better employee morale

CHAPTER 5

SYSTEM DESIGN

Software design is an interactive process through which requirements are translated into a 'Blue Print' for constructing the software. The design is represented at high level of abstraction, a level that can be directly translated to specific data, functional and behavioral requirements.

Preliminary design is concerned with the transformation of requirements into data and software architecture. Detailed design focuses on refinements to the architectural representation that lead to detailed data structure and algorithmic representation for software.

5.1 Introduction to UML

The Unified modeling language (UML) provides a blueprint to Software Engineers and Developers. It is a Language for Specifying, Documenting, Visualizing and constructing the various aspects of a Software System.

UML is an Industry-Standard Modeling Language. It Contains a number of graphical notations and symbols (diagrams) that allow the analyst and designer of a Software Application to describe the architecture of the application in a graphical form.

Definition : UML is a general purpose visual modeling language that is used to

1. Specify
2. Visualize
3. Construct
4. Document

The artifacts of the software system.

5.2. Rules of the UML

The UML has semantic rules for

- NAMES : It will call things, relationships and diagrams
- SCOPE : The content that gives specific meaning to a name
- VISIBILITY : How those names can be seen and used by others
- INTEGRITY : How things properly and consistently relate to Another
- EXECUTION: What it means is to run or simulate a dynamic model

5.3. Building blocks of UML

The vocabulary of the UML encompasses 3 kinds' building blocks

- Things
- Relationships
- Diagrams

5.3.1. Things

Things are the data abstractions that are first class citizens in a model. Things are of 4 types

- Structural things
- Behavioral things
- Grouping things
- An notational things

5.3.2 Relationships

Relationships in the UML are

- Dependency
- Association
- Generalization
- Specialization

5.4 Diagrams

Diagrams in the UML are of 2 types

- Static diagrams
- Dynamic diagrams

Static diagrams

- Class diagram
- Object diagram
- Component diagram
- Deployment diagram

Dynamic diagrams

- Use casediagram
- Sequence diagram
- Collaboration diagram

- State chart diagram
- Activity diagram

5.5 UML Diagrams

A diagram is a graphical representation of a set of elements. The various diagrams in UML are as follows:

5.5.1 CLASS DIAGRAM

A Class diagram shows a set of classes, interfaces, and collaborations and their relationships. Class diagrams address the static design view of a system. Class diagrams that include Active classes address the static process view of a system. A Class is a description of a set of objects that share the same attributes, operations, relationships, and semantics. A Class implements on or more interfaces.

5.5.2 OBJECT DIAGRAM

An Object diagram shows the relationship between a group of objects and their relationships. Object diagrams represent static snapshots of instances of the things found in class diagrams. Object diagram address the static design view or static process view of a system.

5.5.3 USE CASE DIAGRAM

A Use case diagram shows a set of use cases and actors(a special kind of class) and their relationships. Usecase diagrams address the static use case view of a system. These diagrams are especially important in organizing and modeling the behaviors of a system.

5.5.4 SEQUENCE DIAGRAM

A Sequence diagram is a visual representation of a scenario. A sequence diagram shows the various actors in the scenario, and the way they interact with all the subsystems. A Sequence diagram is an interaction diagram that emphasizes the time ordering of messages.

5.5.5 COLLABORATION DIAGRAM

A Collaboration diagram is an interaction diagram that emphasizes the structural organization of the objects that send and receive messages. Collaboration diagram address the dynamic view of a system.

5.5.6 STATE CHART DIAGRAM

A State chart diagram shows how an object dynamically changes its lifetime. A State is a condition or situation in which the object satisfies some condition, does some task, or waits for an event to trigger. A State chart diagram address the dynamic view of the system.

5.5.7 ACTIVITY DIAGRAM

An Activity diagram is a special type of state chart diagram. It usually depicts the flow of events within an object. An Activity diagram addresses the dynamic view of a system. They are especially important in modeling the function of a system and emphasize the flow of control among objects.

5.5.8 COMPONENT DIAGRAM

A Component diagram shows the organizations and dependencies among a set of components. Component diagram address the static implementation view of a system. They are related to class diagrams in that a component typically maps to one or more classes, interfaces, or collaborations.

5.5.9 DEPLOYMENT DIAGRAM

A Deployment diagram shows the architecture of the execution time details of a system. Deployment diagram address the static deployment view of an architecture. They are related to component diagrams in that a node typically encloses one or more components.

1. Use Case Diagram

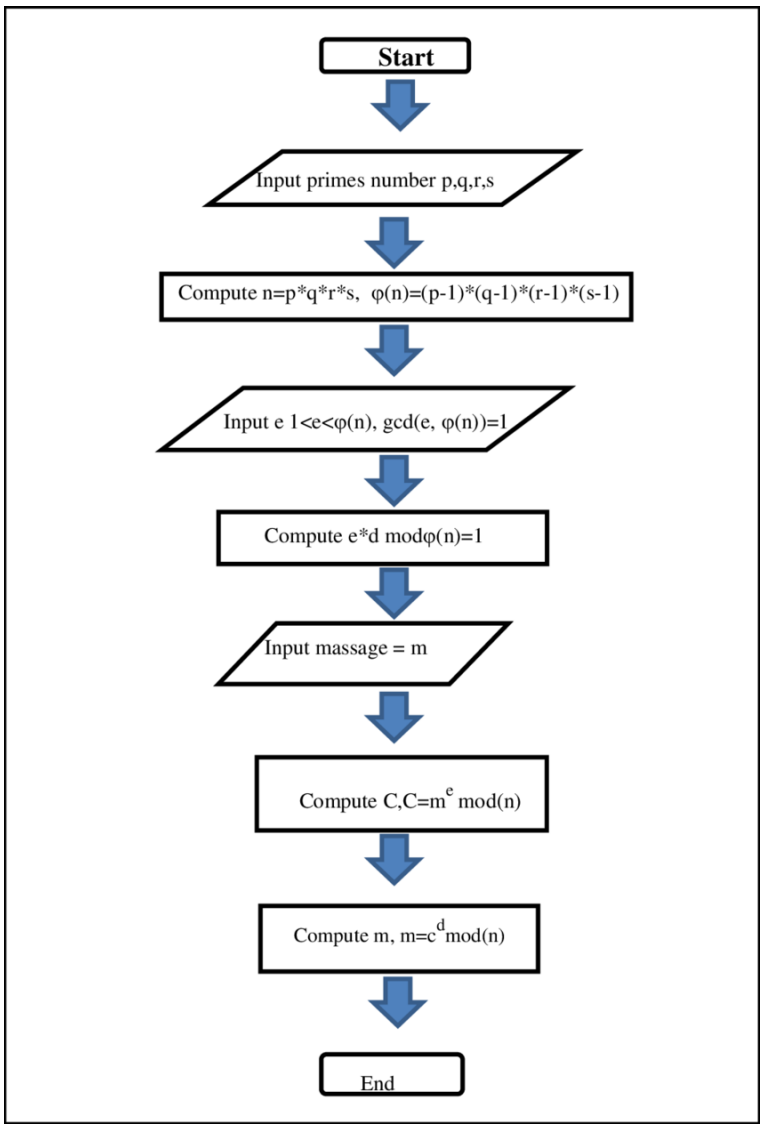
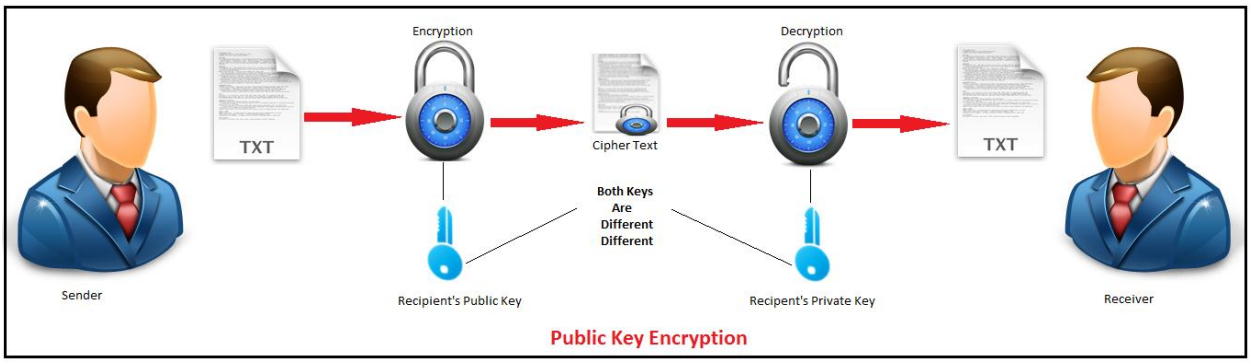


Fig: RSA Encryption and Decryption

4. Activity Diagram :



CHAPTER 6

IMPLEMENTATION

Components are used in Digital Voting System:-

- **Mysql Database**: MySQL is the world's most popular open source database. With its proven performance, reliability and ease-of-use, MySQL has become the leading database choice for web-based applications, used by high profile web properties including Facebook, Twitter, YouTube, Yahoo! and many more. MySQL is a fast, easy-to-use RDBMS being used for many small and big businesses. MySQL is developed, marketed and supported by MySQL AB, which is a Swedish company. MySQL is becoming so popular because of many good reasons.

Webcam Capture : This library allows you to use your build-in or external webcam directly from Java. It's designed to abstract commonly used camera features and support multiple capturing frameworks.

Features

- Simple, thread-safe and non-blocking API,
- No additional software required,
- Supports multiple platforms and various architectures
- Get images from build-in or USB-connected PC webcams,
- Get images from IP / network cameras (as MJPEG or JPEG),
- Offers ready to use motion detector,
- All required JARs Available in Maven Central,
- Offers possibility to expose images as MJPEG stream,
- It is available as Maven dependency or standalone ZIP binary
- Digital Voting System
- Swing component to display video feed from camera,
- Swing component to choose camera (drop down),
- Multiple capturing frameworks are supported:

The newest stable version can be downloaded as separated ZIP binary. This ZIP file contains Webcam Capture API itself and all required dependencies (in libs directory). Click on the below link to download it:

RSA ALGORITHM:

The RSA algorithm was invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman at MIT. The RSA algorithm is the most widely known asymmetric key cryptographic algorithms. The entire RSA algorithm can be performed using three steps:

i. Key generation

ii. Encryption

iii. Decryption

RSA uses two exponents, e and d, in which e is public and d is private. The plaintext is P and C is cipher text, then at encryption side:

$C = Pe \bmod n$

And at decryption side:

$P = Cd \bmod n$

Where, n is a very large number, created during key generation process.

Advanced Encryption Standard(AES):

Advanced Encryption Standard is a symmetric- key encryption algorithm published as FIPS-197 in the Federal Register in December 2001 by the National Institute of Standards and Technology (NIST). It is carefully tested for many security applications. AES algorithm encrypts data with block size of 128-bits. It uses 10, 12 or 14 rounds. The key size may be 128, 192, or 256 bits, depending on the number of rounds.

RGB Color Model:

The RGB color model is based on the work of Thomas Young and Hermann von Helmholtz in the 19th century is a theory of trichromatic color vision, and on James Clerk Maxwell's color triangle that elaborated that theory.

The name of this color model comes from the initials of the three additive primary colors, red, green, and blue. The RGB color model is a color model in which red, green, and blue light are added together in a way to produce a broad array of colors.

Three colored light beams, each of red, green and blue must be superimposed, for forming a color with RGB. Each of the three beams is called a component of that color, and each of them can have an arbitrary intensity, from fully off to fully on, in the mixture as shown in Fig-3.
The full intensity of each component gives a white color while zero intensity for each gives the darkest color that is, no light, considered as black color. The quality of white color depends on the nature of the primary light sources, but if they are properly balanced, the result is a neutral white matching the system's white point. If the intensities for all the color components are same, then the result is a shade of gray, darker or lighter depending on the intensity. When the intensities are different, color shades are also different more or less saturated, depending on the difference of the strongest and weakest of the intensities of the primary colors employed.
In computers, the component values are often stored as integer numbers in the range of 0 to 255, the range that a single 8-bit byte can offer. These are represented as either decimal or hexadecimal numbers..

Color	Decimal Code (R,G,B)
	rgb(255,255,255)
	rgb(255,0,0)
	rgb(0,255,0)
	rgb(0,0,255)
	rgb(255,255,0)
	rgb(0,255,255)
	rgb(255,0,255)
	rgb(192,192,192)
	rgb(128,128,128)
	rgb(128,0,0)

Fig: RGB color model

Comparison of various Algorithm:

A common aim for cryptographic algorithms is to provide confidentiality and authentication. A cryptographic algorithm is considered to be computationally secured if it cannot be broken with standard resources. An efficient cryptosystem

can produce possible results if the key size is comparable to the size of the packet to be transmitted over the network. The algorithm is compared on the basis of parameters like key-length, block-size, security rate and execution time as shown in Table-1:

Factors	DES	AES	RSA	ECC
Contributor	IBM 75	Rijman, Joan	Rivest, Shamir 78	Neal Koblitz, Victor S. Miller
Key Length	56-bits	128, 192 and 256	Based on No. of bits in N=p*q	135-bits
Block Size	64-bits	128 bits	Variants	Variant
Security Rate	Not enough	Excellent	Good	Less
Execution Time	Slow	More fast	Slowest	Fastest

5. IMPLEMENTATION:

First of all every user is assigned with a unique color. The (R, G, B) components of the assigned color are obtained. Next step is to assign unique public key and private key pair for the user. There are calculated using RSA key generations. The sender will know the color values of the receiver to which it wants to send the message. Now the message will be encrypted using public key of the receiver and the receiver's color values are encrypted using the key

6. RESULT:

The system shows result on the basis of inserting messages. It will generate a different graph for different input message. The graph shows a comparison between all four algorithm with respect to time (execution time). For example, consider input1 as "Welcome to SSBT COET, Bambhori", it will generate the graph shown in Chart-1. The graph shows the
time required by each algorithm to execute given input message.

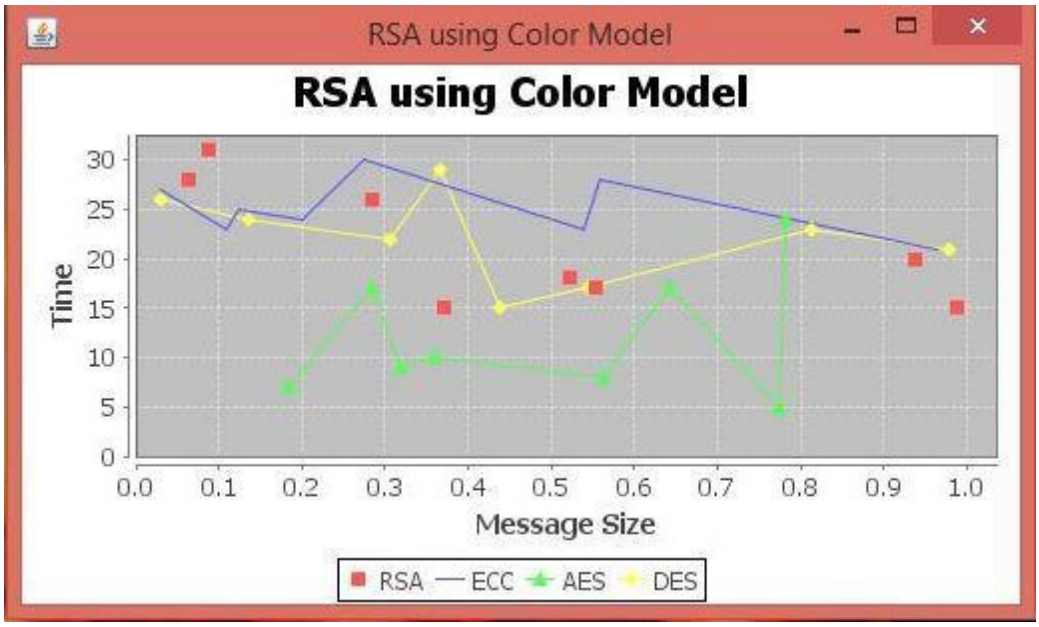


Chart-1: Graph for input2

Considering another example input2 as “Hello, I am Student", it will generate the graph shown in Chart-2. The graph shows some variations from the graph generated by input1.
Hence on the basis of size of message different graph will be generated for different message input. By considering a number of different input graph states that AES works better with the RGB model as it takes less execution time.

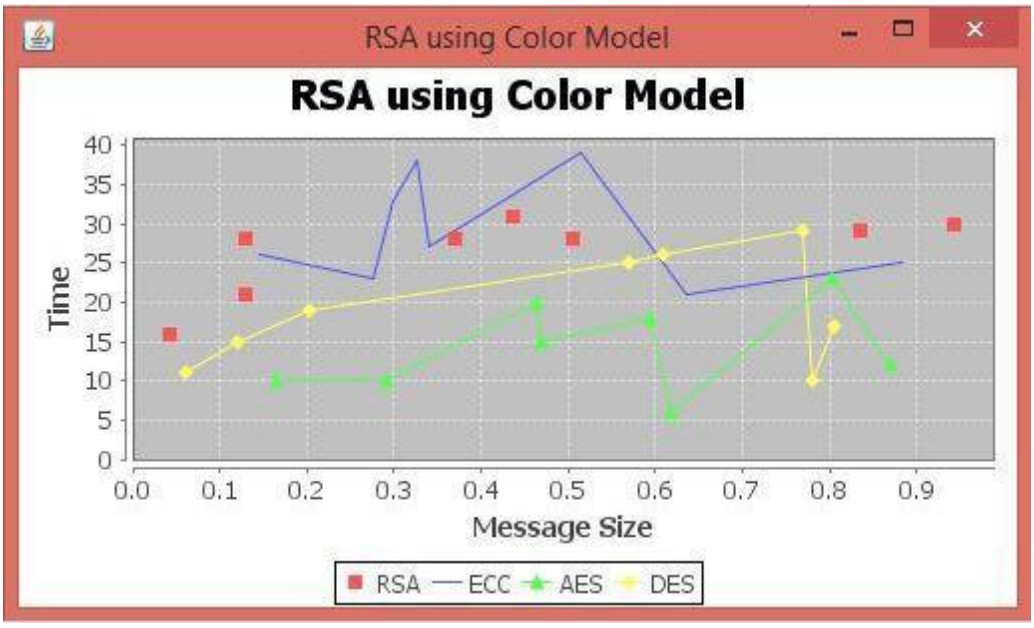


Chart-2: Graph for input2

Hence on the basis of size of message different graph will be generated for different message input. By considering a number of different input graph states that AES works better with the RGB model as it takes less execution time

.

CHAPTER 7

TESTING

7.1. Software Testing

Software testing is a critical element of software quality assurance and represents the ultimate reuse of specification. Design and code testing represents interesting anomaly for the software during earlier definition and development phase, it was attempted to build software from an abstract concept to tangible implementation. The testing phase involves, testing of the development of the system using various techniques such as White Box Testing,Control Structure Testing.

7.2. Testing Techniques

7.2.1 White Box Testing

White box testing is a test case design method that uses the control structure of the procedural design to derive test cases. After performing white box testing it was identified that

- The Leave Recording System (LRS) software guarantees that all independent paths within the modules have been exercised at least once.
- It has been exercised all logical decisions on their true and false sides.
- It was tested to execute all loops at their boundaries and within their Operational bounds
- It was tested for the internal data structures to ensure their validity.

7.2.2 Control Structure Testing

The following tests were conducted and it was noted that the BCBS is performing them well

- Basic path Testing
- Condition Testing
- Data Flow Testing
- Loop Testing

Black box testing methods focuses on the functional requirements of the software by conducting black box testing using the methods Equivalence Partitioning Boundary Value Analysis and Cause-Effect-Graphing techniques.

- Functional validity of LRS checked.

- Checked the isolation of the boundaries of a class.

- The tolerance of the system for the data rates and data volumes

7.3 Testing Strategies

A strategy for software testing must accommodate low-level tests that are necessary to verify that a small source code segment has been correctly implemented as well as high level against customer requirements.

7.3.1 Unit Testing

Unit testing focuses verification on the smaller unit of software design such as form. This is known as form testing. The testing is done individually on each form. Using the unit test plan, prepared in design phase of the system development as a guide, important control paths are tested to uncover within the boundary of the module. In this step, the module is working satisfactorily as a regard to the expected output from the module

7.3.2 Integration Testing

Data can be lost across an interface, one module can have an adverse effect on another sub function**,** when combined, may not produce the desired major function. Integration testing is a systematic

technique for constructing the program structure while at the same time conducting tests to uncover errors associated with the interface. All the modules are combined in the testing step. Then the entire program is as a whole.
Different integrated test plans like top down integration and bottom up integration are tested and different errors found in the system are corrected using them.
Finally, all the combined modules are performed well.

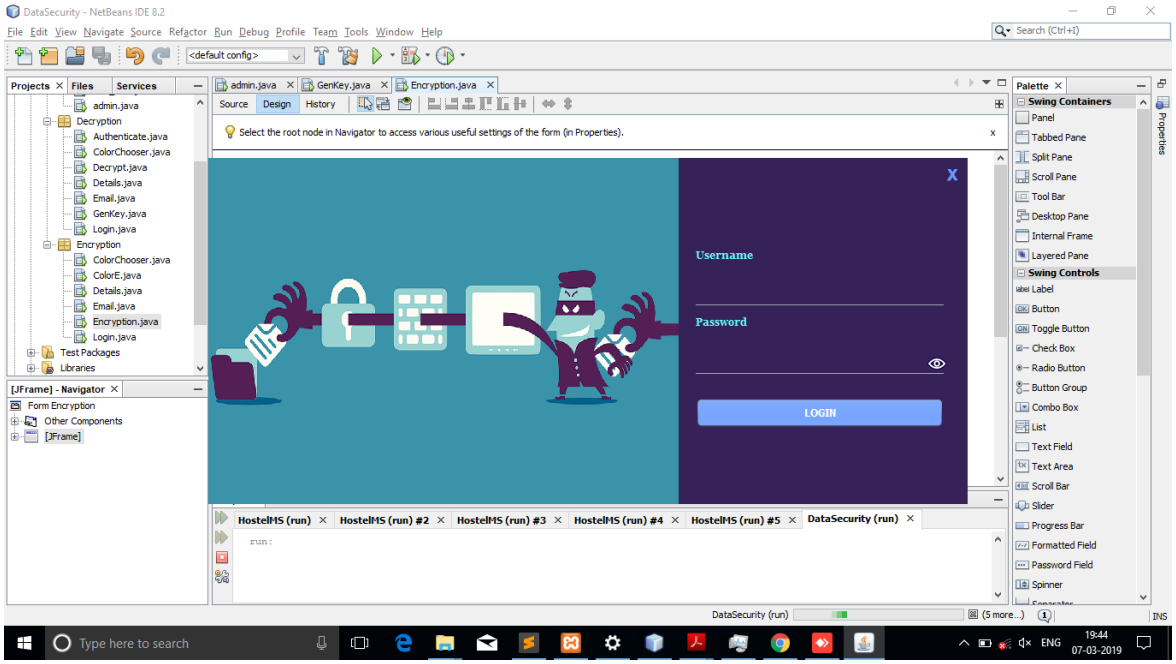
7.3.3 System Testing

Testing the entire system as a whole and checking for its correctness is system testing. The system is listed for dispensaries between the system and its original objectives. This project was effective and efficient

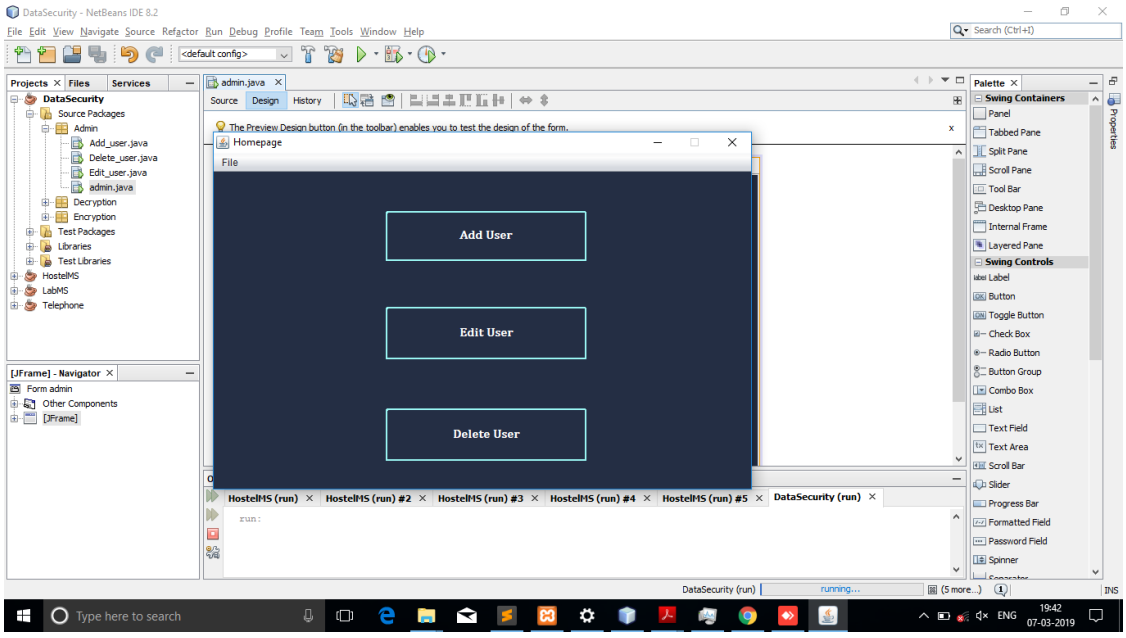
CHAPTER 8

OUTPUT SCREENS

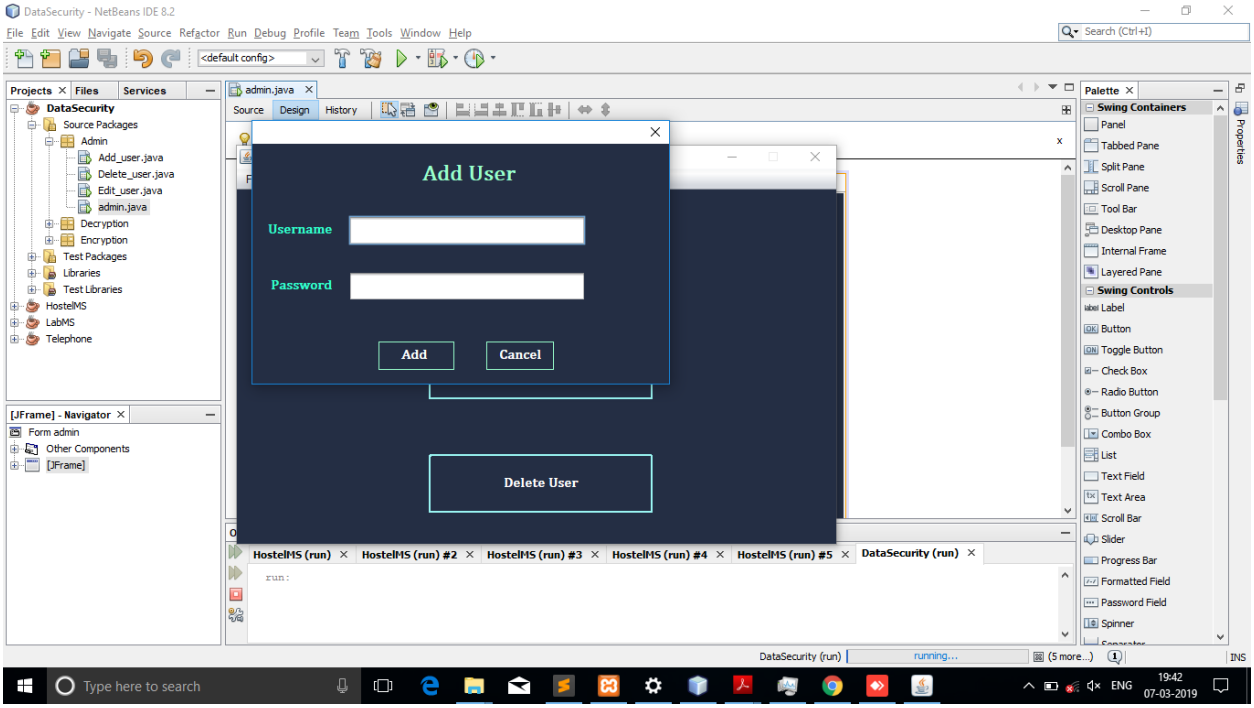
8.1 LOGIN



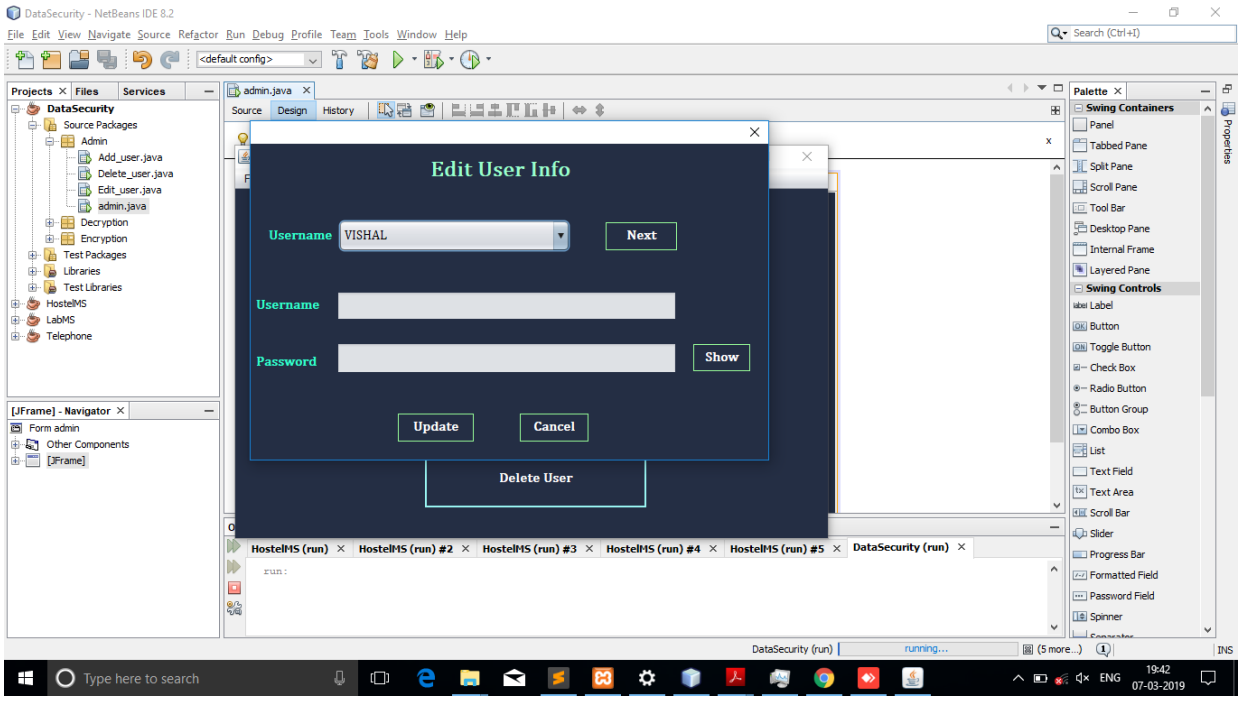
8.2 Home Page:



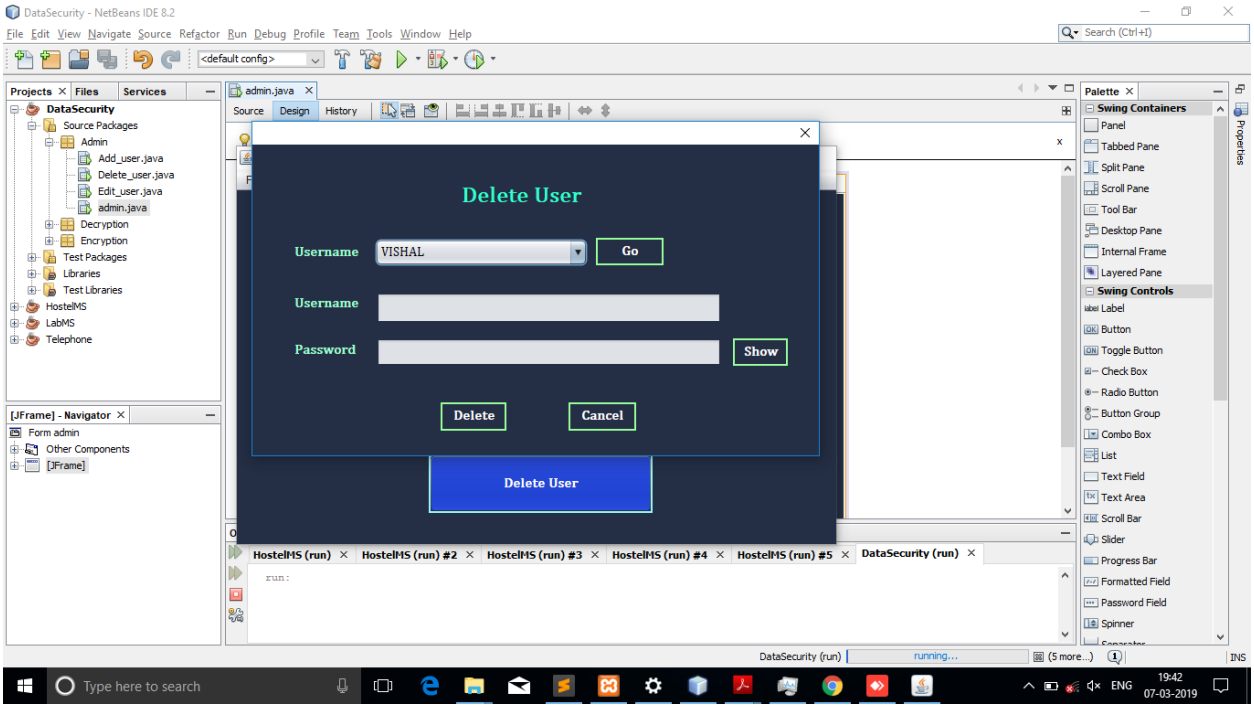
8.3 ADD USER:



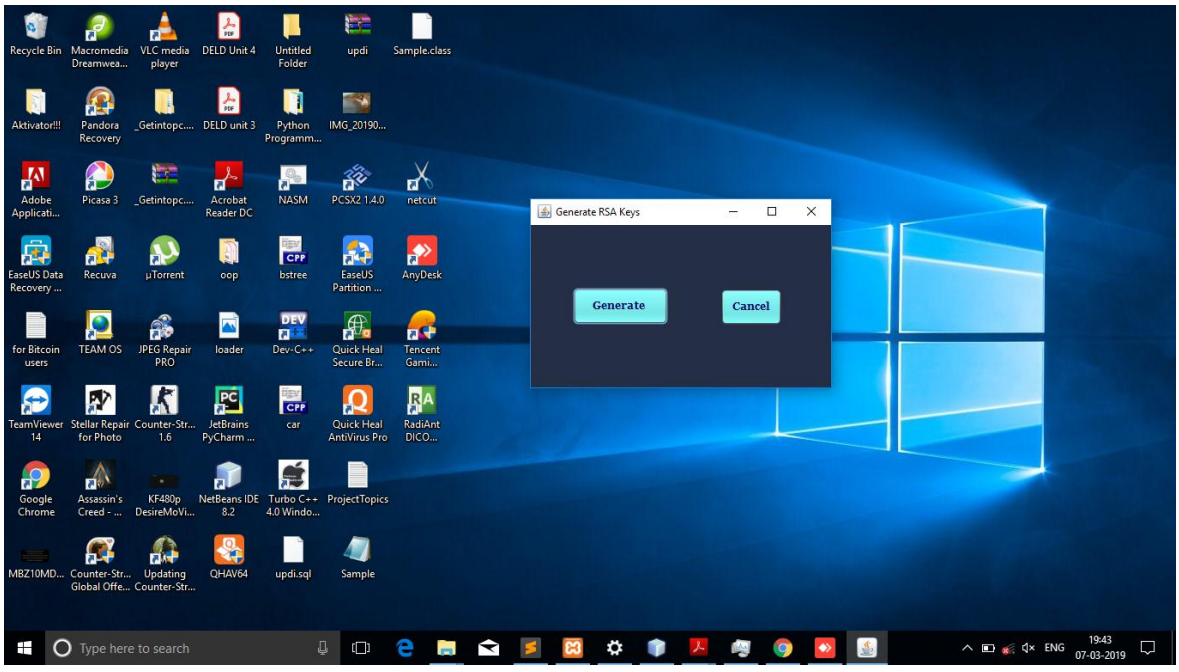
8.4 EDIT USER;



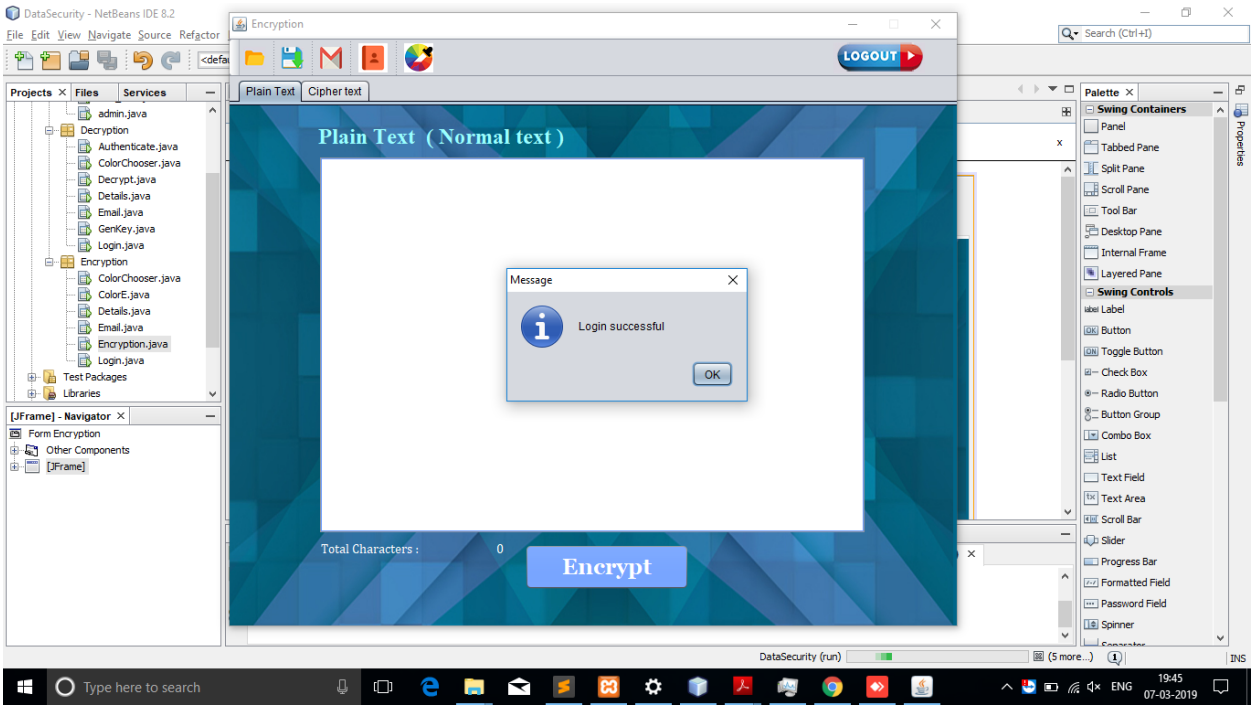
8.5DELETE USER:



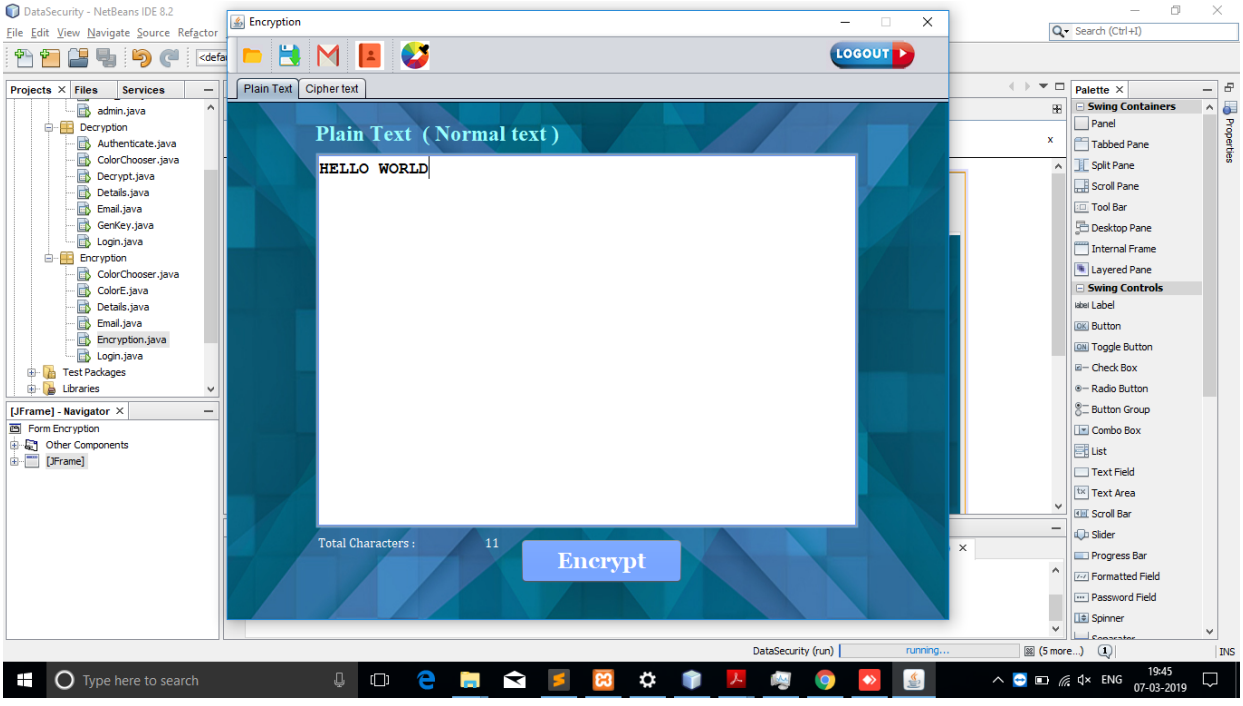
8.6GENRATE THE RSA KEY:



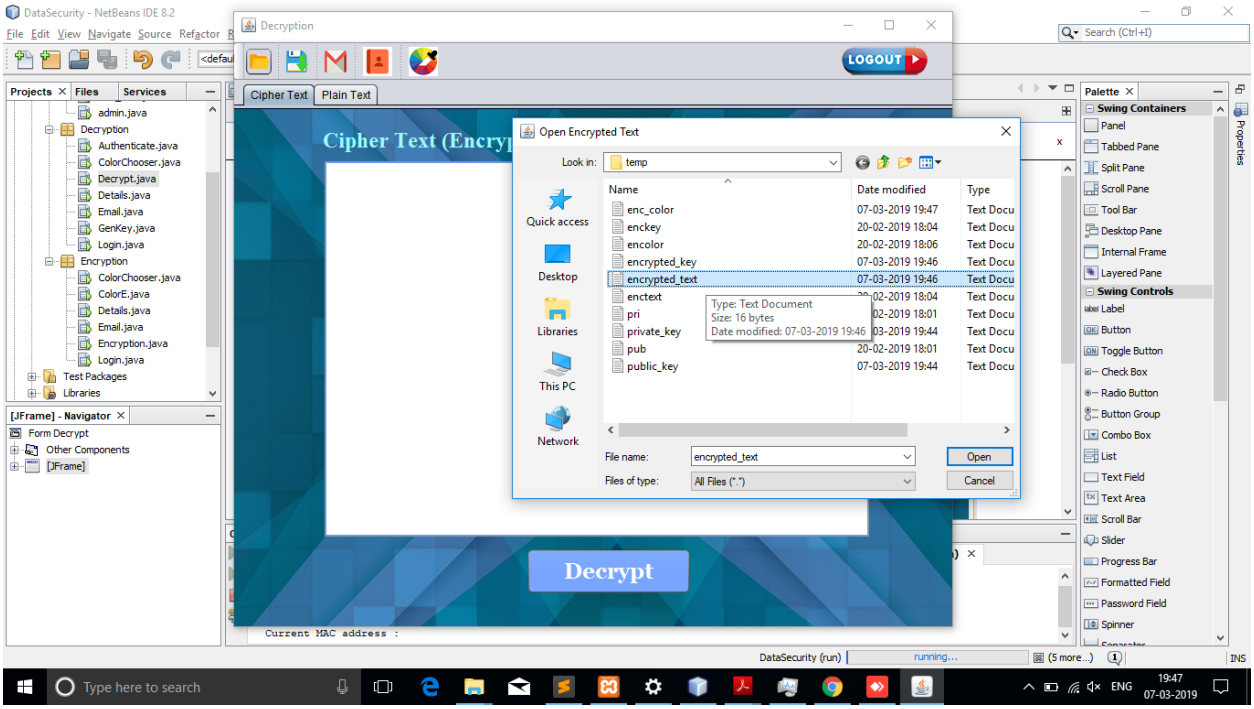
8.7 LOGIN SUCCESFUL:



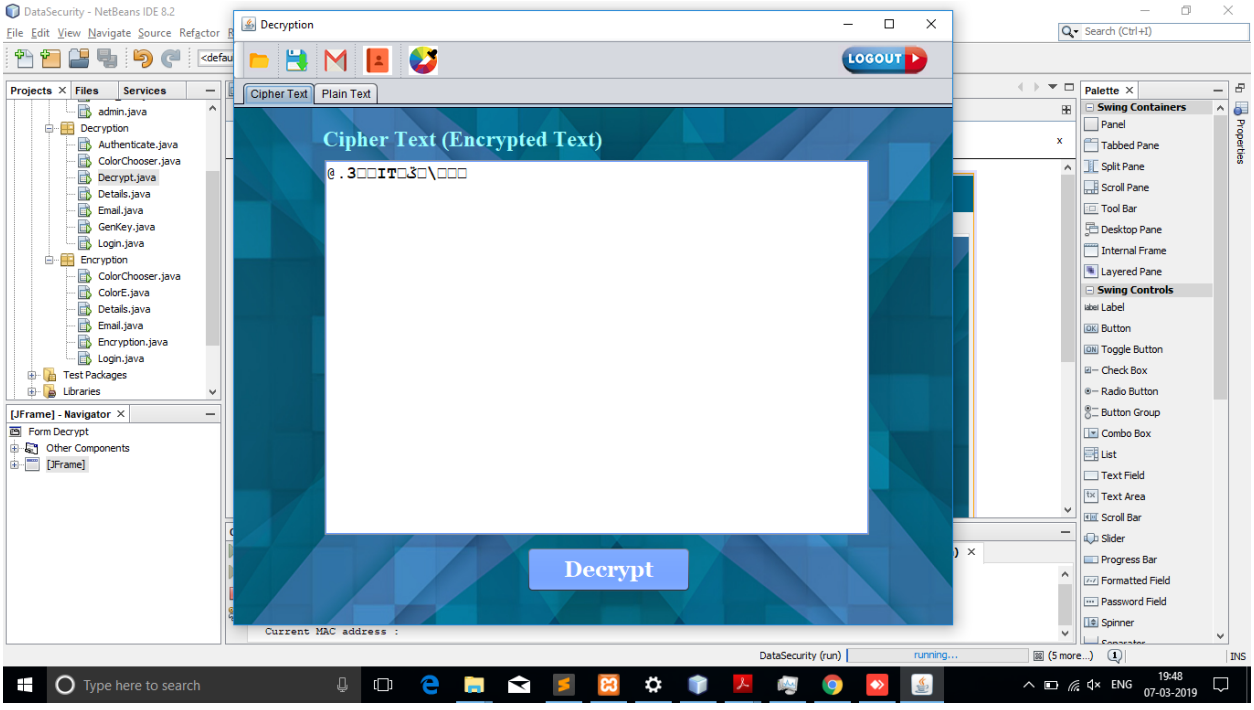
8.8 PLAIN TEXT:



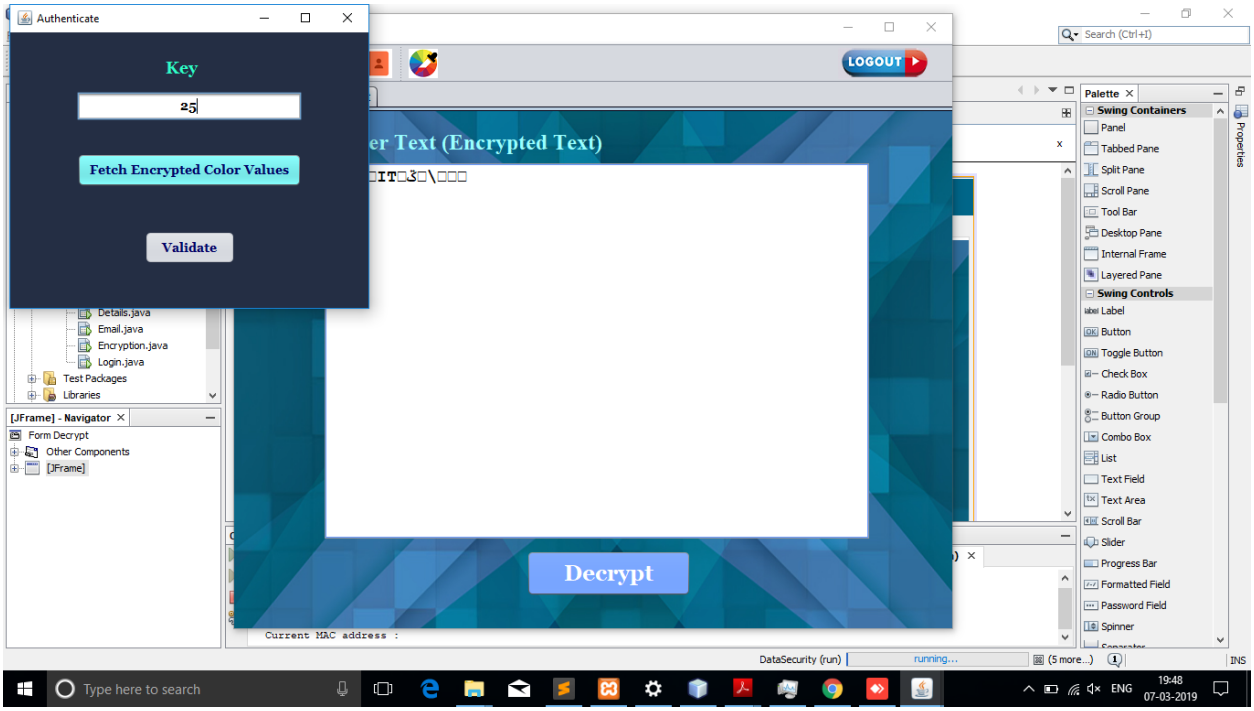
8.9 ENCRYPTION:



8.10CIPHER TEXT:

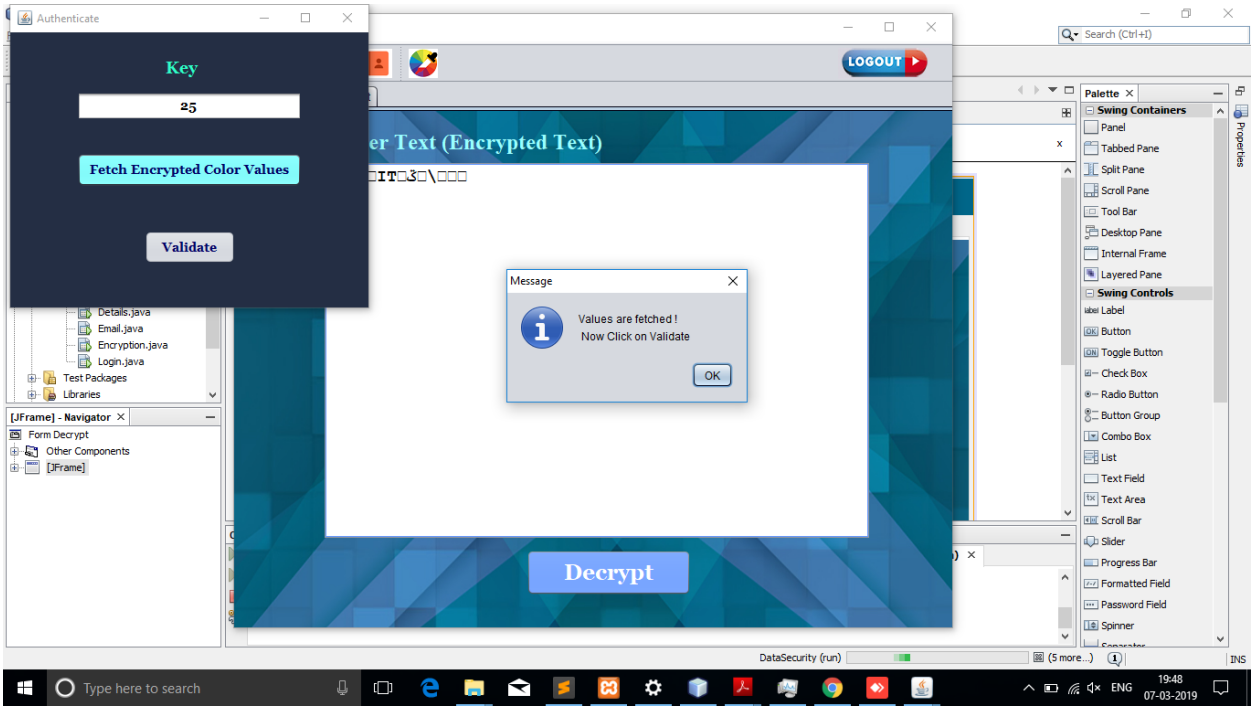


8.11 AUTHENTICATION:

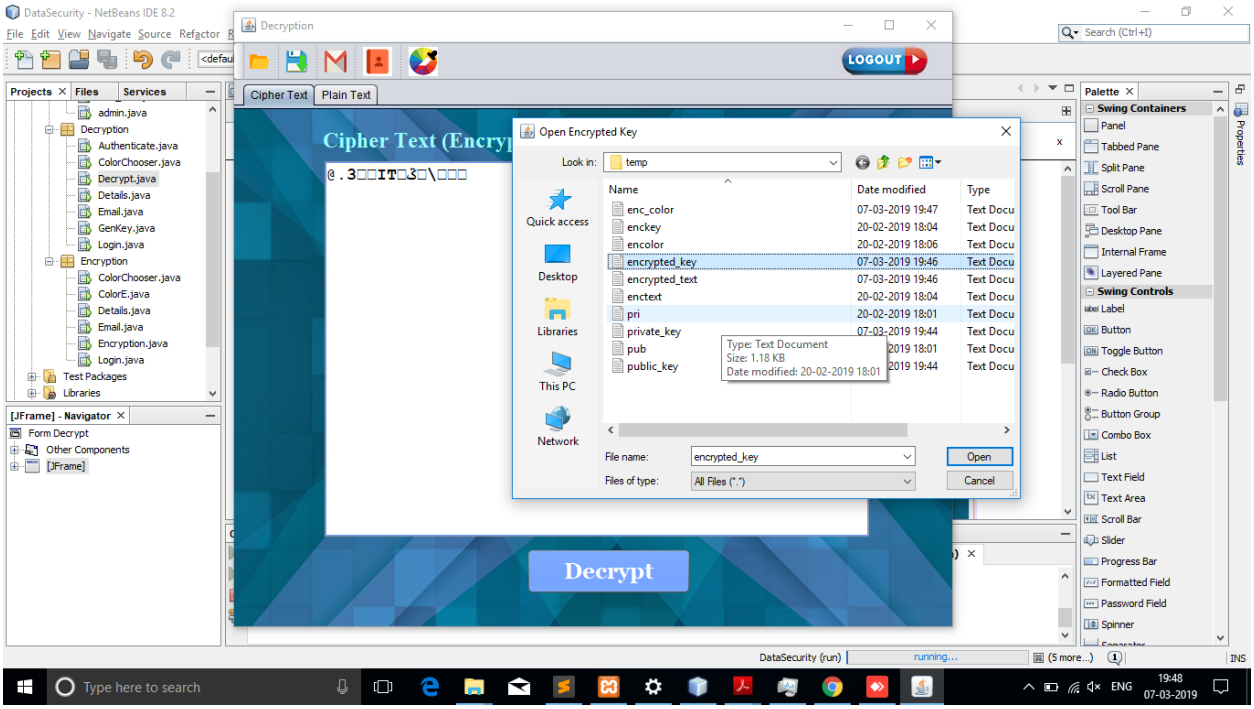


\

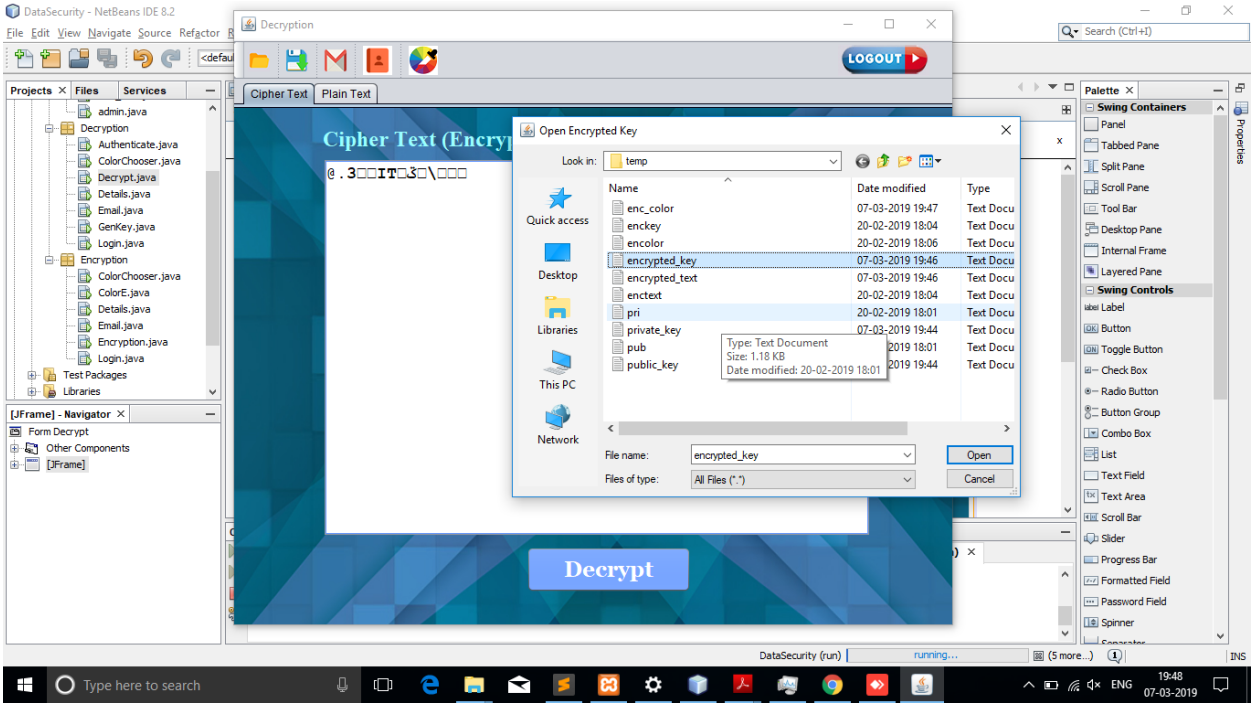
8.12 VALIDATION:

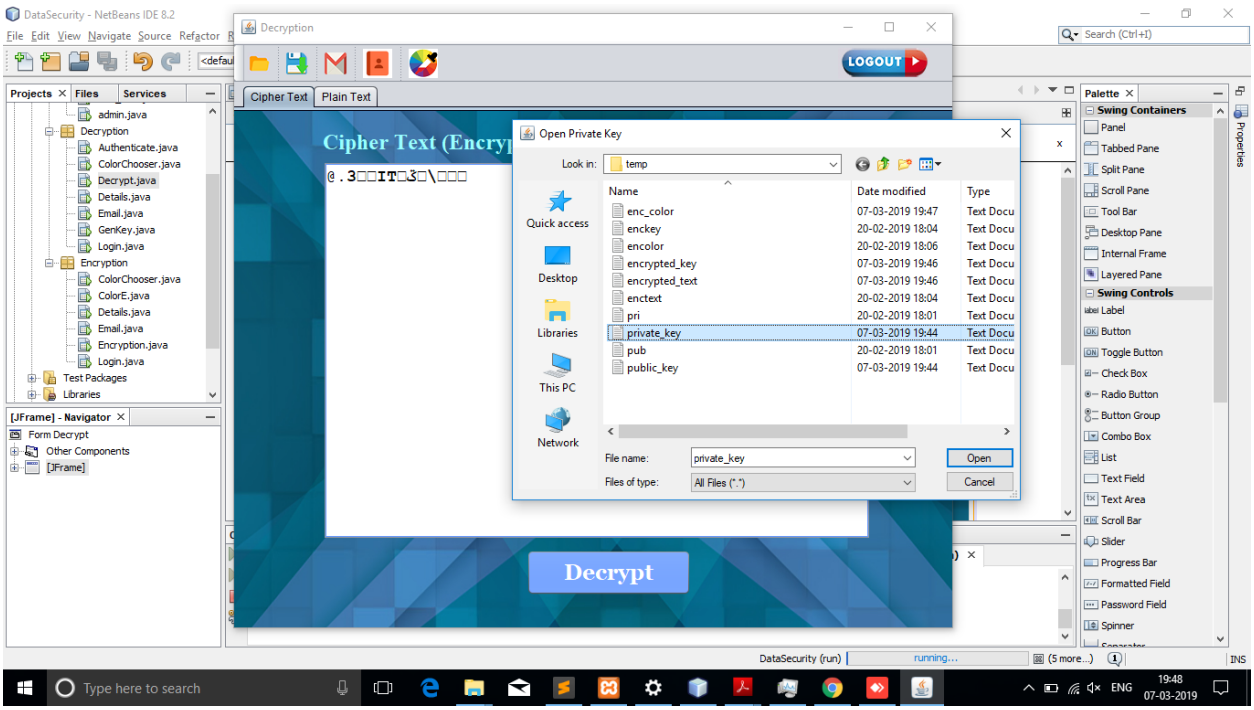


8.12 MATHING KEY:

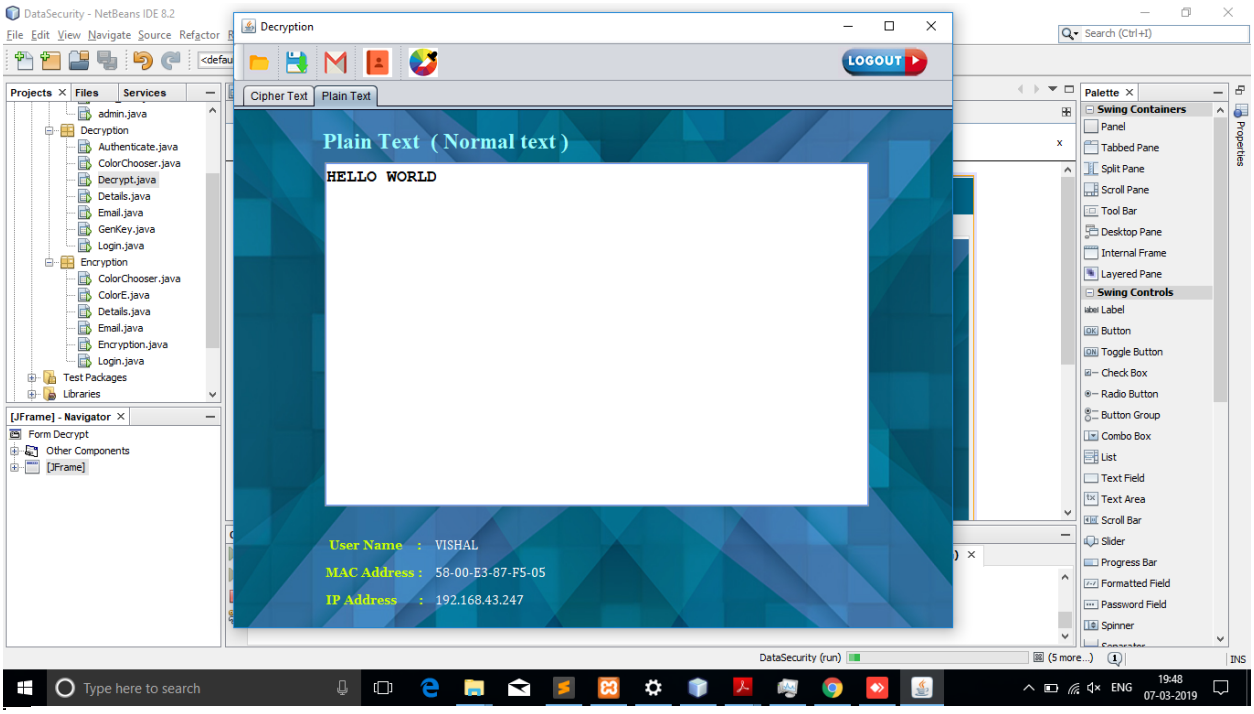


8.13 DECRYPT USING KEY:




DataSecurity - NetBeans IDE 8.2
Decryption
LOGOUT
Cipher Text
Plain Text
Cipher Text (Encry
Open Private Key
Look in: temp
Quick access
Desktop
Libraries
This PC
Network
Name
Date modified
Type
enc_color 07-03-2019 19:47 Text Docu
enckey 20-02-2019 18:04 Text Docu
encolor 20-02-2019 18:06 Text Docu
encrypted_key 07-03-2019 19:46 Text Docu
encrypted_text 07-03-2019 19:46 Text Docu
enctext 20-02-2019 18:04 Text Docu
pri 20-02-2019 18:01 Text Docu
private_key 07-03-2019 19:44 Text Docu
pub 20-02-2019 18:01 Text Docu
public_key 07-03-2019 19:44 Text Docu
File name: private_key
Files of type: All Files (*.*)
Open
Cancel
Decrypt
Projects
Files
Services
Palette
Swing Containers
Swing Controls
[JFrame] - Navigator
Form Decrypt
Other Components
[JFrame]
DataSecurity (run)
running...
Type here to search
ENG
19:48
07-03-2019

8.14 DECRIPT:


DataSecurity - NetBeans IDE 8.2
Decryption
LOGOUT
Cipher Text
Plain Text
Plain Text (Normal text)
HELLO WORLD
User Name : VISHAL
MAC Address : 58-00-E3-87-F5-05
IP Address : 192.168.43.247
Projects
Files
Services
Palette
Swing Containers
Swing Controls
[JFrame] - Navigator
Form Decrypt
Other Components
[JFrame]
DataSecurity (run)
Type here to search
ENG
19:48
07-03-2019

CHAPTER 9

FUTURE SCOPE

CHAPTER 10

APPLICATIONS

CHAPTER 11

CONCLUSION

Encryption algorithm plays very crucial role in communication security. Research work surveyed the performance of AES encryption technique used with RGB Color models to provide security by comparing with different encryption techniques like ECC, DES and RSA algorithms.

The color model and AES encryption technique are the two main factors in proposed system which gives assurance for secured data message transmission which is made available to authorized persons. Based on the texts used and the experimental result, it was concluded that the AES algorithm consumes least encryption and ECC consumes longest encryption time. It also observed that Decryption of AES algorithm is better than other algorithms. From the simulation result, evaluated that AES algorithm is much better than DES, ECC and RSA algorithm. Hence, both authentication and confidentiality are provided with more accuracy.

Future work will focus on compared and analysed existing cryptographic algorithm like AES, DES, ECC and RSA. It will include experiments on image and audio data and focus will be to improve encryption time and decryption time.

Reference

- **Bibliography**

Core Java Volume Two - Herbert Schildt
Database System Concepts - Abraham Silberscharts
Software Engineering - Roger Pressman
Software Engineering & Testing - Khurana
Software Analysis & Design - 1Awad

- **Webliography**

www.mysql.com
www.db4free.com
www.netbeans.com