**ENCYPTOR**

In the Partial Fulfilment of the Requirement for the Award of Degree of

**BACHELOR OF TECHNOLOGY**

By

Avinash Shukla

CU23250462

Aditya Kala

CU23250435

Sachin Kumar Pandey

CU23250474

Saksham saini

CU23250519

**Under the supervision of**

Puja Das



**COER University**, **India**

School of Smart Computing

Department of Computer Science Engineering

**COER University**

Roorkee-247667, Uttarakhand, India

Session:- 2023-2024

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Title** | **Page No.** |
| 1 | Abstract | 4 |
| 2. | Objective and Scope  2.1 Objective  2.2 Scope | 5  6 |
| 3. | Theoretical Background  3.1 Existing System  3.2 Proposed System  3.3 Features  3.4 RSA Algorithm | 7  7  7  8  9 |
| 4. | Feasibility Study  4.1 Economic Feasibility  4.2 Technical Feasibility  4.3 Operational Feasibility | 11  11  12  12 |
| 5. | Problem Definition  5.1 Project Mission  5.2 Target  5.3 Target Users  5.4 Scope and Key Elements | 13  13  13  13  14 |
| 6. | System Design  6.1 System Design  6.2 Data Flow Diagram  6.3 Use Case Diagram | 15  15  15  16 |
| 7. | Source Code | 17 |
| 8. | Screens | 34 |
| 9. | Conclusion | 36 |
| 10. | References | 37 |

Page | 4

**1.ABSTRACT**

The title of our project is “ENCRYPTION AND DECRYPTION”. This project

encrypts and decrypts the textual files by using RSA algorithm. Our aim is todevelop the software named ENCRYPTION AND DECRYPTION that encryptsand decrypts the textual files by using RSA algorithm. Encryption and Decryptionis a strong text and file encryption software for personal and professional security.It protects privacy of our email messages, documents and sensitive files byencrypting them using RSA algorithm to provide high protection againstunauthorized data access.Every day hundreds and thousands of people interact electronically, whether it isthrough emails, e-commerce, etc. through internet. Sending sensitive messagesover the Internet is very dangerous. If you need to send sensitive messages over theInternet, you should send it in the encrypted form. Encryption and Decryptionallows you easily encrypt and decrypt your messages. If you need to send sensitiveinformation via email, simply paste the encrypted text into your email and all therecipients has to do is to decrypt the text.

https://html.scribdassets.com/96uxqyc9ds3q7pma/images/4-7047aa1698.jpg

Page | 5

**2.OBJECTIVE & SCOPE**

**2.1**

**Objective**

The main objective of our project is to encrypt/decrypt the textual files for personal and professional security. Encryption and Decryption protects privacyof our email messages, documents and sensitive files by encrypting them usingRSA algorithm to provide high protection against unauthorized data access.Every day hundreds and thousands of people interact electronically, whether it isthrough emails, e-commerce, etc. through internet. The Internet is comprised ofmillions of interconnected communication and transfer of information around the world. People use emails to correspond with one another .The www is used for online business, data distribution, marketing, research, learning and a my riad of other activities. Sending sensitive messages over the Internet is very dangerous as all emails are transmitted in an unsecured form and anybody - ISP, your boss, etc. can read your emails. If you want to send sensitive information via email, simply paste the encrypted text into your email or attach the [encrypted file,](http://encryption-and-decryption-pro.encryption-and-decryption-com.qarchive.org/) all the recipient has to do is to decrypt your text or file. Encryption and Decryption works with text information and files. Just select what you want to encrypt, and Encryption and Decryption software helps you keep documents, private information and files in a confidential way.

**2.2 Scope**

The scope of our project is presently specific. Both the sender and the receiver must have this software installed on their systems to encrypt/decrypt and compress/decompress the files transmitted between them. This includes all the users who want to interact electronically, whether it is through emails, e-commerce, etc. through internet in order to keep their private information confidential.

* Each step is clearly stated and user will not face any ambiguity in using thesoftware.
* The software provides clarity in its functionality even to naïve users.
* No complexity is involved.

Page | 7

**3.THEORETICAL BACKGROUND**

**3.1 The Existing System**

* As observed the current encryption/decryption softwares doing the encryptionand decryption task are all very complicated in their functionality.

* The method of encryption/decryption and key generation of current system for anew user to understand is complex in nature.

**3.2 The Proposed System**

The proposed system is quiet simple to use. It is not complex in its functionalities.It is easy for a naïve user to use it.If you want to send sensitive information via email, simply paste the encrypted textinto your email or attach the[encrypted file,](http://encryption-and-decryption-pro.encryption-and-decryption-com.qarchive.org/)all the recipient has to do is to decryptyour text or file.Encryption and Decryption works with text information and files.Just select what you want to encrypt, and Encryption and Decryption softwarehelps you keep documents, private information and files in a confidential way.

**3.3 Important features of Encryption and Decryption**

* The system is highly user friendly.
* It uses two different keys (a key pair) for encryption and decryption. These algorithms are called "public-key" because the encryption key can be made public. Anyone can use the public key to encrypt a message, but only the owner of the corresponding private key can decrypt it.

* A message can be encrypted with a private key and decrypted with the corresponding public key.If Alice (or anyone else) can decrypt a message with Bob's public key she knows that the message must have come from Bob because no one else has Bob's private key.

* The system provides security and convenience as private keys never need to be transmitted or revealed to anyone.
* The system provides the integrity of data or information.

* The software provides clarity in its functionality even to naïve users.

**3.4THE ALGORITHM**

The RSA algorithm involves three steps, key generation, encryption and decryption.

**Key Generation**

 RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated in the following way:

1. Choose two distinct large random prime numbers p and q2.
2. Compute n = p q

* n is used as the modulus for both the public and private keys3.

1. Compute the totient : φ(n)=(p-1)(q-1).4.

1. Choose an integer e such that 1<e< φ(n) and e and φ(n) share no factors

other than 1 (i.e. e and φ(n) are co-prime)

* e is released as the public key exponent

5.Compute d to satisfy the congruence relation de≡1(mod φ(n) ; i.e., de=1+kφ(n) for some integer

k.

* d is kept as the private key exponent The public key consists of the modulus n and the public (or encryption) exponent. The private key consists of the modulus n and the private (or decryption)exponent d which must be kept secret.

**Encryption**

Sender A does the following:-

1. Obtains the recipient B's public key (n, e)
2. Represents the plaintext message as a positive integer M
3. Computes the ciphertext C = Me mod n.
4. Sends the ciphertext C to B.

**Decryption**

Recipient B does the following:-1.

Uses his private key (n, d) to compute M = C

d

 mod n.2.

Extracts the plaintext from the message representative M.

Page | 11

**4.FEASIBILITY STUDY**

After investigation it is essential to determine whether the project is feasible or not.In feasibility study is tested whether the system to be developed would be able toaccomplish its task on the working grounds. Its impact was also found to be not

adverse. It was found that the user’s requirements wo

uld be met and the resourceswould be used in an effective manner. In feasibility study the important aspectsrelated to the project were considered like the problem definition and the processfor solution. The cost and benefit analysis was also done.

**4.1 Feasibility Considerations**

To do a feasibility study, the economic, technical and behavioral factors in thesystem development were considered.The three key considerations were as follows:

**4.1.1 Economic Feasibility**

The project developed, Encryption and Decryption was within budget and producing the desired results.The labor or the human ware consisted of thethree group members of our project. The output consisted of getting the

https://html.scribdassets.com/96uxqyc9ds3q7pma/images/11-ed74e40200.jpg

Page | 12

desired results. Thus with the consideration of the inputs, the outputs were

achieved successfully. The project was within limit. The inputs didn’t

overdo the outputs.

**4.1.2 Technical Feasibility**

Technical feasibility revolves around the technical support of the project.The main infrastructure of the project included the project labs in the collegecampus. The systems there were easily able to absorb the new s/w beinginstalled.The project thus was technically feasible. The equipment and the

s/w produced no problem. The project’s technical requirements were met.

The project could be made to work correctly, fulfilling its task, with theexisting s/w and personnel.

**4.1.3 Operational Feasibility**

Operational Feasibility aims to determine the impact of the system on theusers. The system developing has an influence on its users. Our system

“Encryption and Decryption” was new for them but it was simple enough for

any naïve person to understand. The evolution of this new system requiredno special training for the users. Encryption and Decryption was found to befeasible in this regard. The system developed would be user friendly and nocomplexities would be involved in its functionalities.

Page | 13

**5.PROBLEM DEFINITION**

**5.1 Project Mission**

The aim of our project is to develop software named ENCRYPTION ANDDECRYPTION.The project encrypts and decrypts the textual files using RSAalgorithm to maintain the security and integrity of data and information andtoprovide high protection against unauthorized data access.

**5.2 Target**

Our target is the common man who wants to interact electronically, whether it isthrough emails, e-commerce, etc.through internet.Sending sensitive messages overthe Internet is very dangerous.So,our project helps him to interact in a safe andsecure manner in order to keep their private information confidential.

**5.3 Target Users**

The main target users of our project are the people who transmit confidentialinformation via emails or through internet.

https://html.scribdassets.com/96uxqyc9ds3q7pma/images/13-9af2bf31ab.jpg

Page | 14

**5.4 Scope and Key Elements**

The scope of our project is presently specific.Both the sender and the receiver musthave this software installed on their systems to encrypt/decrypt andcompress/decompressthe files transmitted between them.This includes all the userswho want to interact electronically, whether it is through emails, e-commerce,etc.through internet in order to keep their private information confidential.The keyelements of our website include the objectives, plus the following:



The system provides the security and integrity of data or information.



It will provide a more clear and non ambiguous description of the functions.



The system is highly user friendly.



It uses two different keys (a key pair) for encryption and decryption.Thesealgorithms are called "public-key" because the encryption key can be made public. Anyone can use the public key to encrypt a message, butonly theowner of the corresponding private key can decrypt it.



The software provides clarity in its functionality even to naïve users.

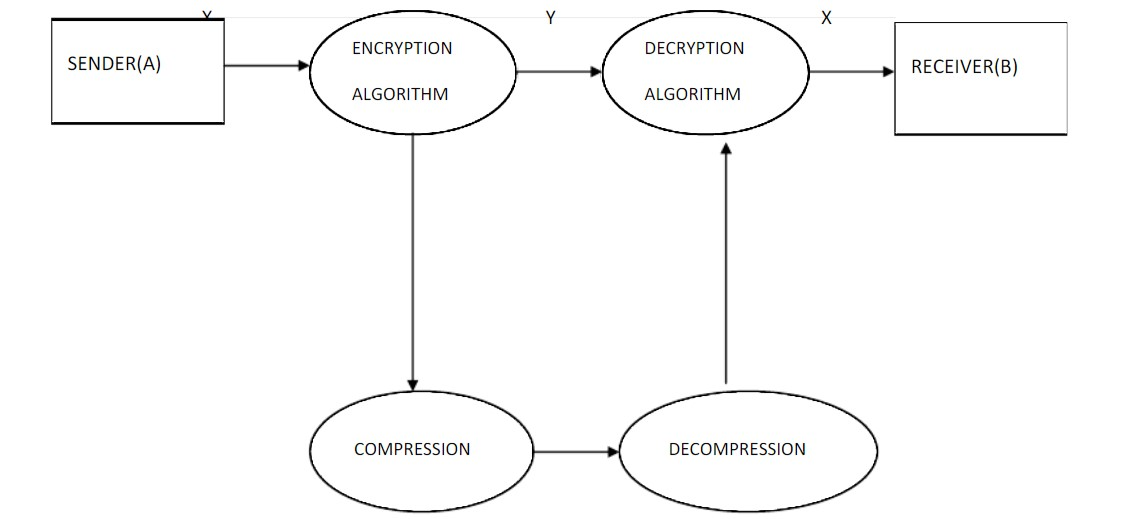
Page | 15

**6. SYSTEM DESIGN**

**6.1 System Design**

Software design sits at the technical kernel of software engineering process and is applied regardless of the development paradigm and the area of application. Once the systemrequirements have been analyzed and specified, system design is the first of the threetechnical activities- design, code and test that are required to build and verify s/w.emphasis is on translating the s/w requirements into design specification. It involves preparing I/P- O/P specifications, making security and control specification, and preparinga logical and physical design work through.

**6.2 Data Flow Diagram**

****

RECEIVER(B)

DECRYPTIONALGORITHMENCRYPTIONALGORITHM

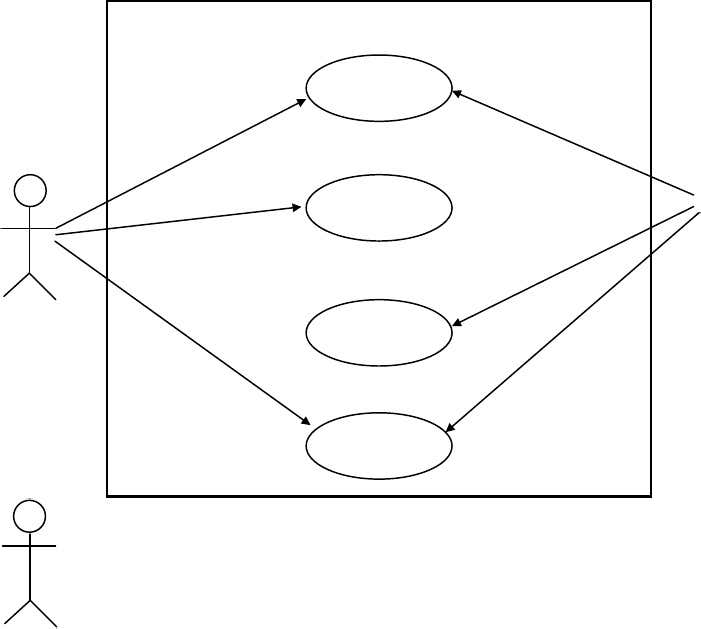
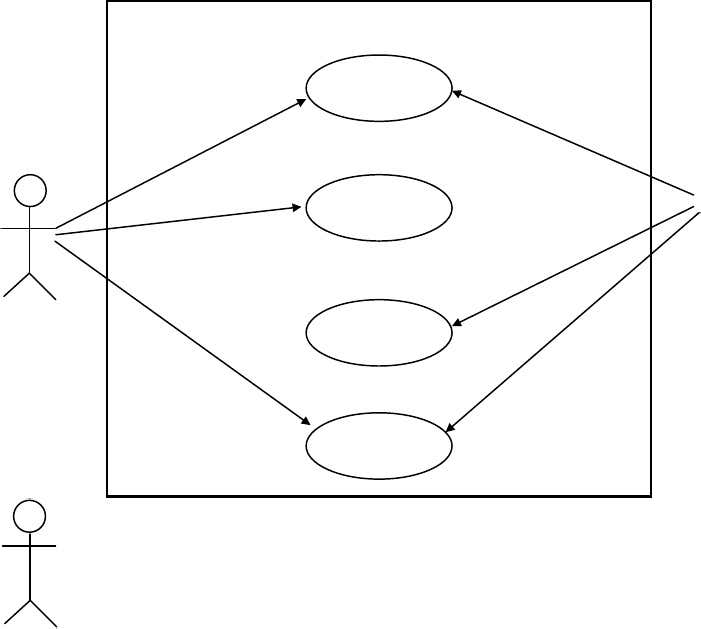
SENDER(A)

COMPRESSION DECOMPRESSION

Page | 16

**6.3 Use Case Diagram**

Select a fileEncryptDecryptExit



Page | 17

**7.SOURCE CODE**

**frmMain.java**

import java.awt.Button;import java.awt.Dimension;import java.awt.Font;import java.awt.Frame;import java.awt.Rectangle;import java.awt.SystemColor;import java.awt.event.ActionEvent;import java.awt.event.ActionListener;import java.awt.event.WindowAdapter;import java.awt.event.WindowEvent; public class frmMain extends Frame{ private Button button1 = new Button(); private Button button2 = new Button(); private Button button3 = new Button(); private Button button4 = new Button(); private Button button5 = new Button(); public frmMain(){try{ jbInit();}catch (Exception e){e.printStackTrace();}} private void jbInit() throws Exception{this.setLayout( null );this.setSize(new Dimension(300, 300));this.setBackground(new java.awt.Color(254, 215, 215));this.setFont(new Font("Dialog", 0, 15));this.setTitle("File Security System");this.addWindowListener(new WindowAdapter() { public void windowClosing(WindowEvent e)

https://html.scribdassets.com/96uxqyc9ds3q7pma/images/17-c6d1fb86fd.jpg

Page | 18

{this\_windowClosing(e);}}); button1.setLabel("Encrypt "); button1.setBounds(new Rectangle(45, 45, 205, 35)); button1.addActionListener(new ActionListener() { public void actionPerformed(ActionEvent e){ button1\_actionPerformed(e);}}); button2.setLabel("Decrypt "); button2.setBounds(new Rectangle(45, 90, 205, 35)); button2.addActionListener(new ActionListener() { public void actionPerformed(ActionEvent e) { button2\_actionPerformed(e);}}); button3.setLabel("Exit"); button3.setBounds(new Rectangle(45, 225, 205, 35)); button3.addActionListener(new ActionListener() { public void actionPerformed(ActionEvent e) {button3\_actionPerformed(e);}});this.add(button1, null);this.add(button2, null);this.add(button3, null);} public static void main(String[] args){(new frmMain()).setVisible(true);} private void this\_windowClosing(WindowEvent e){System.exit(0);} private void button1\_actionPerformed(ActionEvent e){frmEnc f=new frmEnc(this,"File Encryption",true);this.setVisible(false);f.setVisible(true);this.setVisible(true);} private void button2\_actionPerformed(ActionEvent e)

Page | 19

{frmDec f=new frmDec(this,"File Decryption",true);this.setVisible(false);f.setVisible(true);this.setVisible(true);} private void button3\_actionPerformed(ActionEvent e){System.exit(0);}}

**frmEnc.java**

import java.io.\*;import java.security.\*;import java.security.spec.\*;import javax.crypto.\*;import sun.misc.\*;import java.awt.\*;import java.awt.Button;import java.awt.Color;import java.awt.Dialog;import java.awt.Dimension;import java.awt.FileDialog;import java.awt.Font;import java.awt.Frame;import java.awt.Label;import java.awt.Rectangle;import java.awt.Scrollbar;import java.awt.TextField;import java.awt.event.\*;import java.awt.event.ActionListener;import java.awt.event.WindowAdapter;import java.awt.event.WindowEvent;import java.awt.FileDialog;import java.io.\*;import java.util.Arrays; public class frmEnc extends Dialog{ private TextField textField1 = new TextField(); private Label label1 = new Label(); private Button button1 = new Button(); private Button button2 = new Button();

Page | 20

 private Button button3 = new Button(); private Scrollbar scrollbar1 = new Scrollbar(); private Label label5 = new Label(); public frmEnc(Frame parent, String title, boolean modal){super(parent, title, modal);enableEvents(AWTEvent.WINDOW\_EVENT\_MASK);try { jbInit();}catch (Exception e) {e.printStackTrace();}} private void jbInit() throws Exception {this.setSize(new Dimension(629, 235));this.setLayout( null );this.setFont(new Font("Dialog", 0, 16));this.setBackground(new Color(214, 255, 239));this.setBounds(new Rectangle(150, 10, 629, 309));this.addWindowListener(new WindowAdapter() { public void windowClosing(WindowEvent e) {setVisible(false);}});textField1.setBounds(new Rectangle(90, 60, 400, 30));textField1.setFont(new Font("Tahoma", 0, 14));label1.setText("File:");label1.setBounds(new Rectangle(50, 60, 35, 30));label1.setFont(new Font("Tahoma", 0, 16)); button1.setLabel("Browse...."); button1.setBounds(new Rectangle(493, 60, 110, 30)); button1.addActionListener(new ActionListener() { public void actionPerformed(ActionEvent e) {button1\_actionPerformed(e);}}); button2.setLabel("Encrypt"); button2.setBounds(new Rectangle(240, 105, 110, 30)); button2.addActionListener(new ActionListener() { public void actionPerformed(ActionEvent e) { button2\_actionPerformed(e);}}); button3.setLabel("Close"); button3.setBounds(new Rectangle(493, 110, 110, 30)); button3.addActionListener(new ActionListener() { public void actionPerformed(ActionEvent e) { button3\_actionPerformed(e);}});

Page | 21

scrollbar1.setBounds(new Rectangle(120, 200, 480, 30));scrollbar1.setOrientation(0);scrollbar1.setVisibleAmount(5);scrollbar1.setBlockIncrement(5);scrollbar1.setMaximum(255);scrollbar1.setVisible(false);label5.setText("Please wait....");label5.setBounds(new Rectangle(5, 150, 110, 30));label5.setFont(new Font("Tahoma", 0, 16));label5.setVisible(false);this.add(label5, null);this.add(scrollbar1, null);this.add(button3, null);this.add(button2, null);this.add(button1, null);this.add(label1, null);this.add(textField1, null);} protected void processWindowEvent(WindowEvent e) {if (e.getID() == WindowEvent.WINDOW\_CLOSING) {cancel();}super.processWindowEvent(e);}void cancel() { } private void button1\_actionPerformed(ActionEvent e) {FileDialog f=new FileDialog(this,"Select a file");f.setVisible(true);this.textField1.setText(f.getDirectory()+f.getFile());} private void button2\_actionPerformed(ActionEvent e) {MsgBox m=new MsgBox(this,"Confirmation","Are you sure?");m.setVisible(true);//System.out.print(m.type);if(m.type==1) {

**doRSA();**

//Run Scrollbarthis.scrollbar1.setVisible(true);this.label5.setVisible(true);runScrollbar();this.scrollbar1.setVisible(false);this.label5.setVisible(false);

Page | 22

//Done}}

**private**

void doRSA(){try{KeyPair keys=RSAEncryptUtil.generateKey();PublicKey pub=keys.getPublic();PrivateKey pri=keys.getPrivate();RSAEncryptUtil.encryptFile(this.textField1.getText(),this.textField1.getText()+"1",pub);FileInputStream fs=new FileInputStream(this.textField1.getText());int size=fs.available(); byte[] output=new byte[size+10];String str="nnnnnnnnnn"; byte[] pass=str.getBytes(); byte b=105;fs.read(output,10,size);for(int i=0;i<10;i++) {output[i]=pass[i];}for(int i=0;i<output.length;i++) {output[i]=(byte)(output[i]^b);}fs.close();FileOutputStream fo=new FileOutputStream(this.textField1.getText());fo.write(output);fo.close();}catch(Exception ee){}} private void runScrollbar() {try{for(int i=1;i<=255;i++) {this.scrollbar1.setValue(i);Color c=new Color(i,0,0);this.scrollbar1.setBackground(c);Thread.sleep(10);}}catch(Exception ee){}} private void button3\_actionPerformed(ActionEvent e){ this.setVisible(false); }

Page | 23

**frmDec.java**

import java.io.\*;import java.security.\*;import java.security.spec.\*;import javax.crypto.\*;import sun.misc.\*;import java.awt.\*;import java.awt.Button;import java.awt.Color;import java.awt.Dialog;import java.awt.Dimension;import java.awt.FileDialog;import java.awt.Font;import java.awt.Frame;import java.awt.Label;import java.awt.Rectangle;import java.awt.Scrollbar;import java.awt.TextField;import java.awt.event.\*;import java.awt.event.ActionListener;import java.awt.event.WindowAdapter;import java.awt.event.WindowEvent;import java.awt.FileDialog;import java.io.\*;import java.util.Arrays; public class frmDec extends Dialog { private TextField textField1 = new TextField(); private Label label1 = new Label(); private Button button1 = new Button(); private Button button2 = new Button(); private Button button3 = new Button(); private Scrollbar scrollbar1 = new Scrollbar(); private Label label5 = new Label(); public frmDec(Frame parent, String title, boolean modal) {super(parent, title, modal);enableEvents(AWTEvent.WINDOW\_EVENT\_MASK);try { jbInit();}catch (Exception e) { e.printStackTrace(); }

Page | 24

} private void jbInit() throws Exception {this.setSize(new Dimension(629, 235));this.setLayout( null );this.setFont(new Font("Dialog", 0, 16));this.setBackground(new Color(214, 255, 239));this.setBounds(new Rectangle(150, 10, 629, 309));this.addWindowListener(new WindowAdapter() { public void windowClosing(WindowEvent e) {setVisible(false); }});textField1.setBounds(new Rectangle(90, 60, 400, 30));textField1.setFont(new Font("Tahoma", 0, 14));label1.setText("File:");label1.setBounds(new Rectangle(50, 60, 35, 30));label1.setFont(new Font("Tahoma", 0, 16)); button1.setLabel("Browse...."); button1.setBounds(new Rectangle(493, 60, 110, 30)); button1.addActionListener(new ActionListener() { public void actionPerformed(ActionEvent e) { button1\_actionPerformed(e); }}); button2.setLabel("Decrypt"); button2.setBounds(new Rectangle(240, 105, 110, 30)); button2.addActionListener(new ActionListener() { public void actionPerformed(ActionEvent e) { button2\_actionPerformed(e); }}); button3.setLabel("Close"); button3.setBounds(new Rectangle(493, 105, 110, 30)); button3.addActionListener(new ActionListener() { public void actionPerformed(ActionEvent e) { button3\_actionPerformed(e); }});scrollbar1.setBounds(new Rectangle(120, 200, 480, 30));scrollbar1.setOrientation(0);scrollbar1.setVisibleAmount(5);scrollbar1.setBlockIncrement(5);scrollbar1.setMaximum(255);scrollbar1.setVisible(false);label5.setText("Please wait....");label5.setBounds(new Rectangle(5, 150, 110, 30));label5.setFont(new Font("Tahoma", 0, 16));label5.setVisible(false);

Page | 25

this.add(label5, null);this.add(scrollbar1, null);this.add(button3, null);this.add(button2, null);this.add(button1, null);this.add(label1, null);this.add(textField1, null);} protected void processWindowEvent(WindowEvent e) {if (e.getID() == WindowEvent.WINDOW\_CLOSING) {cancel();}super.processWindowEvent(e);}void cancel() { } private void button1\_actionPerformed(ActionEvent e) {FileDialog f=new FileDialog(this,"Select a file");f.setVisible(true);this.textField1.setText(f.getDirectory()+f.getFile());} private void button2\_actionPerformed(ActionEvent e) {MsgBox m=new MsgBox(this,"Confirmation","Are you sure?");m.setVisible(true);//System.out.print(m.type);if(m.type==1) {//Do DecryptiondoRSA();//Run ScrollbarrunScrollbar();//Done}} private void doRSA(){try{KeyPair keys=RSAEncryptUtil.generateKey();PublicKey pri=keys.getPublic();PrivateKey pub=keys.getPrivate();RSAEncryptUtil.encryptFile(this.textField1.getText()+"1",this.textField1.getText()+"e",pri);FileInputStream fs=new FileInputStream(this.textField1.getText());int size=fs.available(); byte[] input=new byte[size];fs.read(input,0,size); byte[] output=new byte[size-10];

Page | 26

 byte[] pass=new byte[10]; byte b=105;for(int i=0;i<10;i++) { pass[i]=(byte)(input[i]^b);}for(int i=10;i<size;i++) {output[i-10]=(byte)(input[i]^b);}this.scrollbar1.setVisible(true);this.label5.setVisible(true);runScrollbar();this.scrollbar1.setVisible(false);this.label5.setVisible(false);FileOutputStream fo=new FileOutputStream(this.textField1.getText());fo.write(output);fo.close();fs.close();}catch(Exception ee){}} private void runScrollbar() {try{for(int i=1;i<=255;i++) {this.scrollbar1.setValue(i);Color c=new Color(i,0,0);this.scrollbar1.setBackground(c);Thread.sleep(10);}}catch(Exception ee){}} private void button3\_actionPerformed(ActionEvent e) {this.setVisible(false);}}

**RSAEncryptUtil**

import java.io.\*;import java.security.\*;import java.security.spec.\*;import javax.crypto.\*;import sun.misc.\*;