IMPLEMENTATION OF RSA ALGORITHM

R V S TEJA KRISHNA(17MIS7085)

K VARUN TEJA(17MIS7156)

```
/*
 * To change this license header, choose License Headers in Project Properties.
 * To change this template file, choose Tools | Templates
 * and open the template in the editor.
 */
package rsa;
import java.util.*;
import java.math.*;



/**
 *
 * @author krish
 */
public class RSAimplementation extends javax.swing.JFrame {

    /**
     * Creates new form RSAimplementation
     */
```

```
public RSAimplementation() {
    initComponents();
}

/**
 * This method is called from within the constructor to initialize the form.
 * WARNING: Do NOT modify this code. The content of this method is always
 * regenerated by the Form Editor.
 */
@SuppressWarnings("unchecked")
// <editor-fold defaultstate="collapsed" desc="Generated Code">
private void initComponents() {

    jPanel1 = new javax.swing.JPanel();
    jLabel1 = new javax.swing.JLabel();
    jLabel2 = new javax.swing.JLabel();
    m1 = new javax.swing.JTextField();
    jLabel3 = new javax.swing.JLabel();
    p1 = new javax.swing.JTextField();
    jLabel4 = new javax.swing.JLabel();
    p2 = new javax.swing.JTextField();
    jButton1 = new javax.swing.JButton();
    jLabel5 = new javax.swing.JLabel();
```

```
        e1 = new javax.swing.JTextField();
        jLabel6 = new javax.swing.JLabel();
        d1 = new javax.swing.JTextField();
        jButton2 = new javax.swing.JButton();
        edv = new javax.swing.JLabel();


setDefaultCloseOperation(javax.swing.WindowConstants.EXIT_ON_CLOSE);


        jPanel1.setBackground(new java.awt.Color(0, 0, 0));
        jPanel1.setLayout(new org.netbeans.lib.awtextra.AbsoluteLayout());


        jLabel1.setFont(new java.awt.Font("Times New Roman", 1, 24)); // NOI18N
        jLabel1.setForeground(new java.awt.Color(0, 204, 51));
        jLabel1.setText("IMPLEMENTATION OF RSA ALGORITHM...|");
        jPanel1.add(jLabel1, new org.netbeans.lib.awtextra.AbsoluteConstraints(80,
20, -1, -1));


        jLabel2.setFont(new java.awt.Font("Times New Roman", 1, 18)); // NOI18N
        jLabel2.setForeground(new java.awt.Color(0, 204, 0));
        jLabel2.setText("Enter the message:");
        jPanel1.add(jLabel2, new org.netbeans.lib.awtextra.AbsoluteConstraints(150,
80, -1, -1));
```

```
        m1.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                m1ActionPerformed(evt);
            }
        });
        jPanel1.add(m1, new org.netbeans.lib.awtextra.AbsoluteConstraints(320, 80, 200, -1));

        jLabel3.setFont(new java.awt.Font("Times New Roman", 1, 18)); // NOI18N
        jLabel3.setForeground(new java.awt.Color(0, 204, 0));
        jLabel3.setText("Enter the 1st prime number:");
        jPanel1.add(jLabel3, new org.netbeans.lib.awtextra.AbsoluteConstraints(70, 120, 240, -1));
        jPanel1.add(p1, new org.netbeans.lib.awtextra.AbsoluteConstraints(320, 120, 200, -1));

        jLabel4.setFont(new java.awt.Font("Times New Roman", 1, 18)); // NOI18N
        jLabel4.setForeground(new java.awt.Color(0, 204, 0));
        jLabel4.setText("Enter the 2nd prime number:");
        jPanel1.add(jLabel4, new org.netbeans.lib.awtextra.AbsoluteConstraints(63, 160, -1, -1));
        jPanel1.add(p2, new org.netbeans.lib.awtextra.AbsoluteConstraints(320, 160, 200, -1));
```

```
        jButton1.setBackground(new java.awt.Color(0, 0, 0));
        jButton1.setFont(new java.awt.Font("Times New Roman", 1, 18)); // NOI18N
        jButton1.setForeground(new java.awt.Color(0, 204, 0));
        jButton1.setText("Encrypt and Decrypt");
        jButton1.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                jButton1ActionPerformed(evt);
            }
        });
        jPanel1.add(jButton1, new
org.netbeans.lib.awtextra.AbsoluteConstraints(240, 210, -1, -1));

        jLabel5.setFont(new java.awt.Font("Times New Roman", 1, 18)); // NOI18N
        jLabel5.setForeground(new java.awt.Color(0, 204, 0));
        jLabel5.setText("Encrypted:");
        jPanel1.add(jLabel5, new org.netbeans.lib.awtextra.AbsoluteConstraints(60,
280, -1, -1));
        jPanel1.add(e1, new org.netbeans.lib.awtextra.AbsoluteConstraints(160, 280,
160, -1));

        jLabel6.setFont(new java.awt.Font("Times New Roman", 1, 18)); // NOI18N
        jLabel6.setForeground(new java.awt.Color(0, 204, 0));
        jLabel6.setText("Decrypted:");
```

```
        jPanel1.add(jLabel6, new org.netbeans.lib.awtextra.AbsoluteConstraints(340,
280, -1, -1));

        jPanel1.add(d1, new org.netbeans.lib.awtextra.AbsoluteConstraints(440, 280,
160, -1));


        jButton2.setBackground(new java.awt.Color(0, 0, 0));

        jButton2.setFont(new java.awt.Font("Times New Roman", 1, 14)); // NOI18N

        jButton2.setForeground(new java.awt.Color(0, 204, 0));

        jButton2.setText("Clear");

        jButton2.addActionListener(new java.awt.event.ActionListener() {

            public void actionPerformed(java.awt.event.ActionEvent evt) {

                jButton2ActionPerformed(evt);

            }

        });

        jPanel1.add(jButton2, new
org.netbeans.lib.awtextra.AbsoluteConstraints(300, 330, -1, -1));


        edv.setFont(new java.awt.Font("Times New Roman", 1, 14)); // NOI18N

        edv.setForeground(new java.awt.Color(0, 204, 0));

        jPanel1.add(edv, new org.netbeans.lib.awtextra.AbsoluteConstraints(320,
380, -1, -1));


        javax.swing.GroupLayout layout = new
javax.swing.GroupLayout(getContentPane());
```

```
        getContentPane().setLayout(layout);
        layout.setHorizontalGroup(
            layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addComponent(jPanel1, javax.swing.GroupLayout.DEFAULT_SIZE, 693, Short.MAX_VALUE)
        );
        layout.setVerticalGroup(
            layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addComponent(jPanel1, javax.swing.GroupLayout.DEFAULT_SIZE, 411, Short.MAX_VALUE)
        );

        pack();
    }// </editor-fold>

    private void m1ActionPerformed(java.awt.event.ActionEvent evt) {
        // TODO add your handling code here:
    }

    private void jButton2ActionPerformed(java.awt.event.ActionEvent evt) {
        // TODO add your handling code here:
        m1.setText(null);
```

```
    p1.setText(null);
    p2.setText(null);
    e1.setText(null);
    d1.setText(null);
}

private void jButton1ActionPerformed(java.awt.event.ActionEvent evt) {
    // TODO add your handling code here:
    String message=m1.getText();
    int msg= Integer.parseInt(message);
    double c;
    BigInteger msgback;
    int p=Integer.parseInt(p1.getText());
    int q=Integer.parseInt(p2.getText());
    /*for(int ch=2;ch<=p/2;++ch){
        if(p%ch==0 && q%ch==0){
            break;
        }
        else{
            e1.setText("Check Primes");
            d1.setText("Check Primes");
        }
    }*/
```

```
int n=p*q;
int z=(p-1)*(q-1);
int e,d=0;
for(e=2;e<z;e++){
    if(gcd(e,z)==1){
        break;
    }
}
//System.out.println("the value of e is:"+e);
for(int i=0;i<=9;i++){
    int x=1+(i*z);
    if(x%e==0){
        d=x/e;
        break;
    }
}
//System.out.println("the value  of d is:"+d);
c=(Math.pow(msg,e))%n;
e1.setText(Double.toString(c));
BigInteger N = BigInteger.valueOf(n);
BigInteger C = BigDecimal.valueOf(c).toBigInteger();
msgback = (C.pow(d)).mod(N);
String s1=msgback.toString();
```

```
        d1.setText(s1);
        edv.setText("The Value of e is "+e+"        the value of d is "+d);
    }

    static int gcd(int e,int z){
        if(e==0){
            return z;
        }
        else{
            return gcd(z%e,e);
        }
    }
    /**
     * @param args the command line arguments
     */
    public static void main(String args[]) {
        /* Set the Nimbus look and feel */
        //<editor-fold defaultstate="collapsed" desc=" Look and feel setting code (optional) ">
        /* If Nimbus (introduced in Java SE 6) is not available, stay with the default look and feel.
         * For details see http://download.oracle.com/javase/tutorial/uiswing/lookandfeel/plaf.html
         */
```

```
        try {
            for (javax.swing.UIManager.LookAndFeelInfo info :
javax.swing.UIManager.getInstalledLookAndFeels()) {
                if ("Nimbus".equals(info.getName())) {
                    javax.swing.UIManager.setLookAndFeel(info.getClassName());
                    break;
                }
            }
        } catch (ClassNotFoundException ex) {

java.util.logging.Logger.getLogger(RSAimplementation.class.getName()).log(java
.util.logging.Level.SEVERE, null, ex);
        } catch (InstantiationException ex) {

java.util.logging.Logger.getLogger(RSAimplementation.class.getName()).log(java
.util.logging.Level.SEVERE, null, ex);
        } catch (IllegalAccessException ex) {

java.util.logging.Logger.getLogger(RSAimplementation.class.getName()).log(java
.util.logging.Level.SEVERE, null, ex);
        } catch (javax.swing.UnsupportedLookAndFeelException ex) {

java.util.logging.Logger.getLogger(RSAimplementation.class.getName()).log(java
.util.logging.Level.SEVERE, null, ex);
        }
        //</editor-fold>
```

```
    /* Create and display the form */
    java.awt.EventQueue.invokeLater(new Runnable() {
        public void run() {
            new RSAimplementation().setVisible(true);
        }
    });
}

// Variables declaration - do not modify
private javax.swing.JTextField d1;
private javax.swing.JTextField e1;
private javax.swing.JLabel edv;
private javax.swing.JButton jButton1;
private javax.swing.JButton jButton2;
private javax.swing.JLabel jLabel1;
private javax.swing.JLabel jLabel2;
private javax.swing.JLabel jLabel3;
private javax.swing.JLabel jLabel4;
private javax.swing.JLabel jLabel5;
private javax.swing.JLabel jLabel6;
private javax.swing.JPanel jPanel1;
private javax.swing.JTextField m1;
```

```
    private javax.swing.JTextField p1;
    private javax.swing.JTextField p2;
    // End of variables declaration
}
```