IT8761 – Security Laboratory

Reshma Ramesh Babu

312217104129

Exercise 5

Aim: To implement Advanced Encryption Standard (AES) in java.

Code:

```
import java.util.*;

import java.io.*;

import javax.crypto.Cipher;

importjavax.crypto.spec.SecretKeySpec;
import java.security.*;

class AES {

private static SecretKeySpecsecretKey;

private static byte[] key;

public static void setKey(String myKey)

{

        MessageDigest sha = null;
        try {

                key = myKey.getBytes("UTF-8"); sha =
                MessageDigest.getInstance(“SHA-1");

                key = sha.digest(key); key =
                Arrays.copyOf(key, 16); secretKey = new
                SecretKeySpec(key, "AES");

            } catch (Exception e)

                {

                        e.printStackTrace();
```

```
                    }

}

public static String encrypt(String strToEncrypt, String secret)

{ try {

                    setKey(secret);
                    Cipher cipher =
          Cipher.getInstance("AES/ECB/PKCS5Padding");
                    cipher.init(Cipher.ENCRYPT_MODE, secretKey); return
          Base64.getEncoder().encodeToString(
          cipher.doFinal(strToEncrypt.getBytes("UTF-8")) );

               } catch (Exception e) {
          System.out.println("Error while encrypting: " + e.toString());

} return null; } public static String decrypt(String strToDecrypt,

String secret) { try {      setKey(secret);

Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5PADDING");
cipher.init(Cipher.DECRYPT_MODE, secretKey); return new
String(cipher.doFinal(Base64.getDecoder().decode(strToDecrypt)));

} catch (Exception e) {
System.out.println("Error while decrypting: " + e.toString());

} return null;

}

public String aes(String secretKey, String originalString, int ch) { String

encryptedString, decryptedString; if (ch == 1) { encryptedString =

AES.encrypt(originalString, secretKey); return encryptedString; } else if (ch == 2) {

decryptedString = AES.decrypt(originalString, secretKey); return decryptedString; }

return ""; }

}
```

```
/** *

* @author reshma
*/ public class GUI extends

javax.swing.JFrame {

   /**
* Creates new form GUI
    */
public GUI() { 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">//GEN-
BEGIN:initComponents private void initComponents() {

jLabel1 = new javax.swing.JLabel(); jLabel2 = new javax.swing.JLabel(); jLabel3
= new javax.swing.JLabel(); jTextField1 = new javax.swing.JTextField();
jTextField2 = new javax.swing.JTextField(); jButton1 = new
javax.swing.JButton(); jButton2 = new javax.swing.JButton(); jTextField3 = new
javax.swing.JTextField(); jLabel4 = new javax.swing.JLabel();
```

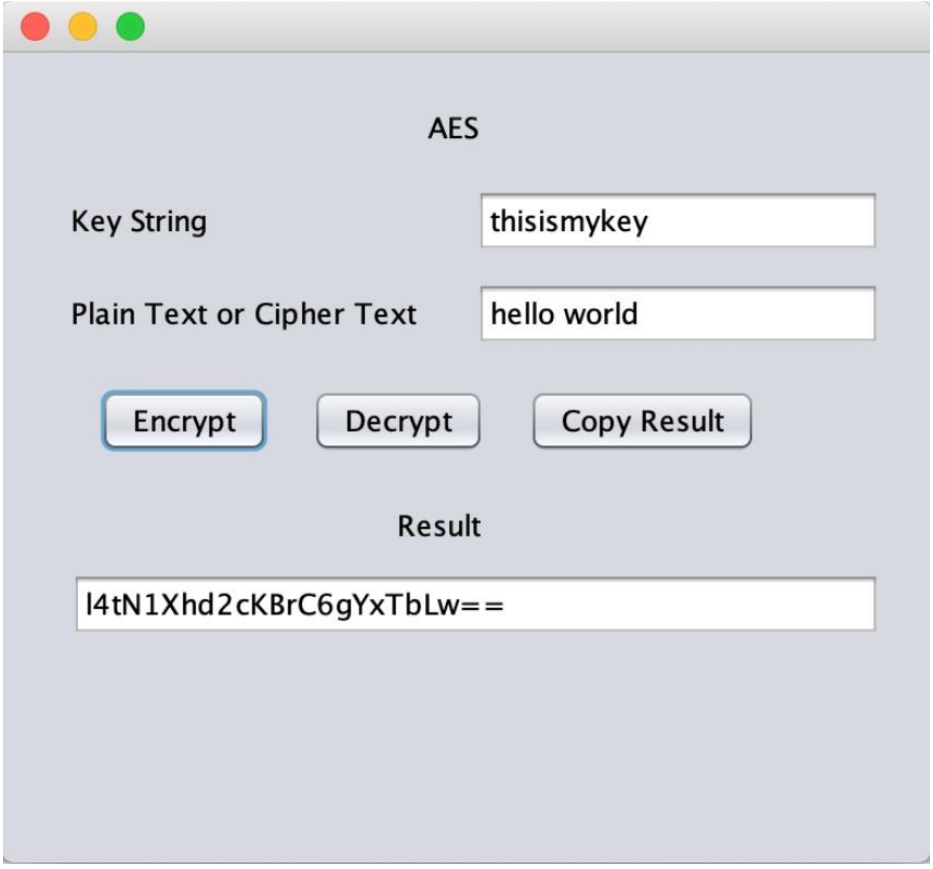
```
jButton3 = new javax.swing.JButton();
setDefaultCloseOperation(javax.swing.WindowConstants.EXIT_ON_CLOSE)
; jLabel1.setText("AES"); jLabel2.setText("Key String");
jLabel3.setText("Plain Text or Cipher Text");

jTextField1.addActionListener(new java.awt.event.ActionListener() { public void
actionPerformed(java.awt.event.ActionEvent evt) {

           jTextField1ActionPerformed(evt);
       } });

jButton1.setText("Encrypt");
jButton1.addActionListener(new java.awt.event.ActionListener() {
```

```
public void actionPerformed(java.awt.event.ActionEvent
evt) { jButton1ActionPerformed(evt);

} });

jButton2.setText("Decrypt"); jButton2.addActionListener(new
java.awt.event.ActionListener() {

public void actionPerformed(java.awt.event.ActionEvent
evt) { jButton2ActionPerformed(evt);

} });

jTextField3.addActionListener(new java.awt.event.ActionListener() { public void
actionPerformed(java.awt.event.ActionEvent evt) {

          jTextField3ActionPerformed(evt);
       }
}); jLabel4.setText("Result");

jButton3.setText("Copy Result");
jButton3.addActionListener(new
java.awt.event.ActionListener() {

public void actionPerformed(java.awt.event.ActionEvent
evt) { jButton3ActionPerformed(evt);

} });

   /*
     Generated Swing Layout Code
*/

private void jButton1ActionPerformed(java.awt.event.ActionEvent evt) {
//GENFIRST:event_jButton1ActionPerformed // TODO add your handling
code here:
String k = jTextField1.getText().toString();

String o = jTextField2.getText().toString();
```

```
AES aes = new AES(); jTextField3.setText(aes.aes(k, o, 1)); }//GEN-

LAST:event_jButton1ActionPerformed
```

```
private void jButton2ActionPerformed(java.awt.event.ActionEvent evt) {
//GENFIRST:event_jButton2ActionPerformed // TODO add your handling
code here:
String k = jTextField1.getText().toString();

String o = jTextField2.getText().toString(); AES aes = new AES();
jTextField3.setText(aes.aes(k, o, 2));

}//GEN-LAST:event_jButton2ActionPerformed

private void jButton3ActionPerformed(java.awt.event.ActionEvent evt) {
//GENFIRST:event_jButton3ActionPerformed // TODO add your handling
code here:
String string = jTextField3.getText().toString(); jTextField2.setText(string);

}//GEN-LAST:event_jButton3ActionPerformed

/**
 * @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)
"> 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(GUI.class.getName()).log(java.util.logging.Level.S
EVERE, null, ex);

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

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

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

}

//</editor-fold>

   /* Create and display the form */
java.awt.EventQueue.invokeLater(new Runnable() { public void run() {

new GUI().setVisible(true); }

4

}); }

// Variables declaration - do not modify//GEN-BEGIN:variables

private javax.swing.JButton jButton1;
private javax.swing.JButton jButton2;
private javax.swing.JButton jButton3;
private javax.swing.JLabel jLabel1;
private javax.swing.JLabel jLabel2;
private javax.swing.JLabel jLabel3;
private javax.swing.JLabel jLabel4;
private javax.swing.JTextField jTextField1; private javax.swing.JTextField jTextField2;
private javax.swing.JTextField jTextField3; // End
of variables declaration//GEN-END:variables

}
```

Output:



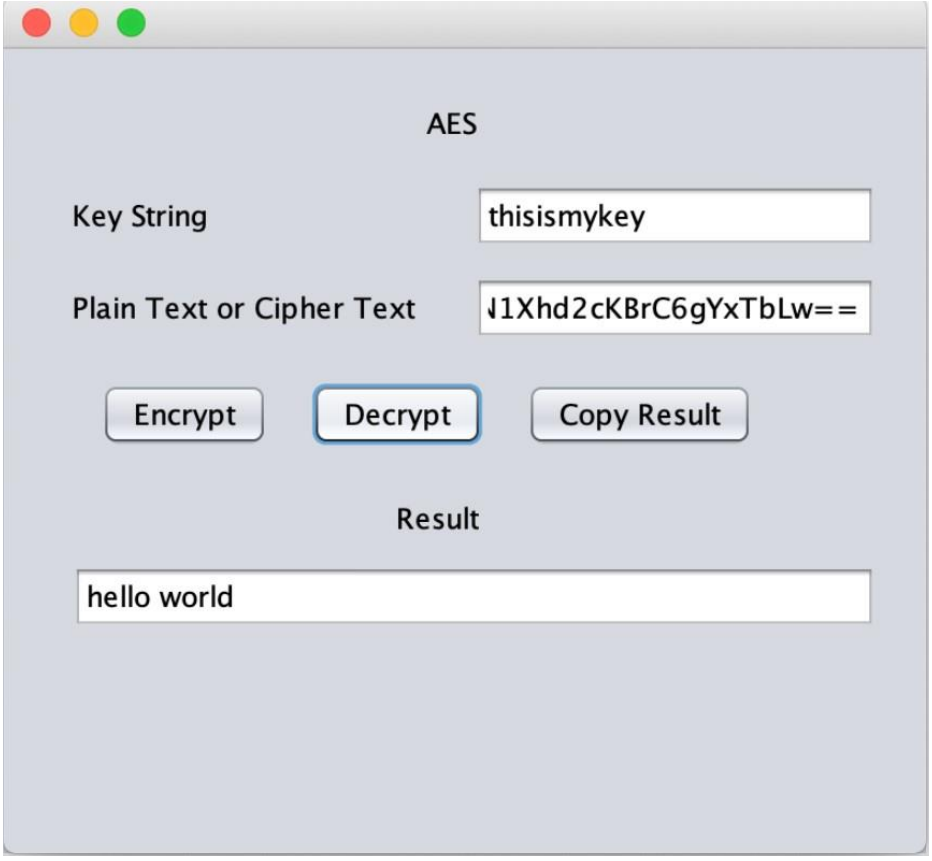
AES

Key String: thisismykey

Plain Text or Cipher Text: hello world

Result

l4tN1Xhd2cKBrC6gYxTbLw==



Key String: thisismykey

Plain Text or Cipher Text: 1Xhd2cKBrC6gYxTbLw==

Result: hello world