Contents

[1 Nối chuỗi. 1](#_Toc136986418)

[2 thuật toán Caesar 1](#_Toc136986419)

[3 thuật toán Vigenere 4](#_Toc136986420)

[4 thuật toán Play Fair 10](#_Toc136986421)

[5 thuật toán DES 16](#_Toc136986422)

[6 thuật toán 3DES 20](#_Toc136986423)

[7 thuật toán RAILFENCE 25](#_Toc136986424)

[8 thuật toán AES. 28](#_Toc136986425)

[9 RSA(Form)\* 32](#_Toc136986426)

[10 thuật toán RSA(nhức đầu). 33](#_Toc136986427)

[11 Thuật toán SHA. 35](#_Toc136986428)

[12 Thuật toán HASH MD5. 36](#_Toc136986429)

[13 File code Thuật toán RSA nâng cao(code java). 38](#_Toc136986430)

[13.1 Skey\_RSA. 38](#_Toc136986431)

[13.2 ENC\_RSA. 39](#_Toc136986432)

[13.3 DEC\_RSA. 39](#_Toc136986433)

1. Nối chuỗi.

String user = txtusername.getText();

String pass = txtpass.getText();

txtchuoi.setText("Username:"+user+" "+"Password: "+ pass);

1. thuật toán Caesar

private void btnmahoaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

int k= Integer.valueOf(this.txtkhoa.getText());

String br=this.txtvanban.getText();

this.txtmahoa.setText(mahoa(br,k));

}

private void btnGhiFileActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

try {

BufferedWriter bw = null;

String fileName = "D:\\THBMTT\\Dulieu.txt";

String s= txtmahoa.getText();

bw = new BufferedWriter(new FileWriter(fileName));

bw.write(s);

bw.close();

JOptionPane.showMessageDialog(null, "Đa ghi File thanh công!!!");

}

catch (IOException ex)

{

Logger.getLogger(class1.class.getName()).log(Level.SEVERE, null, ex);

}

}

private void btngiaimaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

int k= Integer.valueOf(this.txtkhoa.getText());

String br=this.txtmahoa.getText();

this.txtvanban.setText(mahoa(br,-k));

}

private void btnMoFileActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

try {

BufferedReader br = null;

String fileName = "D:\\THBMTT\\Dulieu.txt";

br = new BufferedReader(new FileReader(fileName));

StringBuffer sb = new StringBuffer();

JOptionPane.showMessageDialog(null, "Đa mơ File thanh công!!!");

char[] ca = new char[5];

while (br.ready()){

int len = br.read(ca);

sb.append(ca, 0, len);

}

br.close();

System.out.println("Du lieu la:" + " "+sb);

String chuoi = sb.toString();

txtvanban.setText(chuoi);

}

catch (IOException ex)

{

Logger.getLogger(class1.class.getName()).log(Level.SEVERE, null, ex);

}

}

char mahoakt(char c, int k)

{

if(!Character.isLetter(c)) return c;

return (char) ((((Character.toUpperCase(c) - 'A') + k) %26 +26) %26+'A');

}

private String mahoa(String br, int k){

String kq="";

int n=br.length();

for(int i=0;i<n;i++)

kq+=mahoakt(br.charAt(i),k);

return kq;

}

1. thuật toán Vigenere

public class class2 extends javax.swing.JFrame {

int vig[][];

/\*\*

\* Creates new form class2

\*/

public class2() {

initComponents();

vig= new int[26][26];

for(int i = 0; i<26; i++)

for(int j=0;j<26;j++)

vig[i][j] = (i+j)%26;

}

/\*\*

\* 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() {

jLabel1 = new javax.swing.JLabel();

jLabel2 = new javax.swing.JLabel();

jLabel3 = new javax.swing.JLabel();

jScrollPane1 = new javax.swing.JScrollPane();

txtbanma = new javax.swing.JTextArea();

btnMaHoa = new javax.swing.JButton();

btnGiaiMa = new javax.swing.JButton();

txtbanro = new javax.swing.JTextField();

txtkhoa = new javax.swing.JTextField();

setDefaultCloseOperation(javax.swing.WindowConstants.EXIT\_ON\_CLOSE);

jLabel1.setText("Ban ro:");

jLabel2.setText("Khoa:");

jLabel3.setText("Ban ma:");

txtbanma.setColumns(20);

txtbanma.setRows(5);

jScrollPane1.setViewportView(txtbanma);

btnMaHoa.setText("Ma hoa");

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

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

btnMaHoaActionPerformed(evt);

}

});

btnGiaiMa.setText("Giai ma");

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

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

btnGiaiMaActionPerformed(evt);

}

});

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

getContentPane().setLayout(layout);

layout.setHorizontalGroup(

layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)

.addGroup(layout.createSequentialGroup()

.addContainerGap()

.addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING, false)

.addGroup(layout.createSequentialGroup()

.addComponent(jLabel3)

.addGap(18, 18, 18)

.addComponent(jScrollPane1, javax.swing.GroupLayout.PREFERRED\_SIZE, 386, javax.swing.GroupLayout.PREFERRED\_SIZE))

.addGroup(layout.createSequentialGroup()

.addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)

.addComponent(jLabel1)

.addComponent(jLabel2))

.addGap(27, 27, 27)

.addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)

.addComponent(txtkhoa)

.addComponent(txtbanro))))

.addContainerGap(47, Short.MAX\_VALUE))

.addGroup(layout.createSequentialGroup()

.addGap(107, 107, 107)

.addComponent(btnMaHoa)

.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED, javax.swing.GroupLayout.DEFAULT\_SIZE, Short.MAX\_VALUE)

.addComponent(btnGiaiMa)

.addGap(89, 89, 89))

);

layout.setVerticalGroup(

layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)

.addGroup(layout.createSequentialGroup()

.addGap(20, 20, 20)

.addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.BASELINE)

.addComponent(jLabel1)

.addComponent(txtbanro, javax.swing.GroupLayout.PREFERRED\_SIZE, javax.swing.GroupLayout.DEFAULT\_SIZE, javax.swing.GroupLayout.PREFERRED\_SIZE))

.addGap(40, 40, 40)

.addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.BASELINE)

.addComponent(jLabel2)

.addComponent(txtkhoa, javax.swing.GroupLayout.PREFERRED\_SIZE, javax.swing.GroupLayout.DEFAULT\_SIZE, javax.swing.GroupLayout.PREFERRED\_SIZE))

.addGap(30, 30, 30)

.addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)

.addComponent(jScrollPane1, javax.swing.GroupLayout.PREFERRED\_SIZE, 143, javax.swing.GroupLayout.PREFERRED\_SIZE)

.addComponent(jLabel3))

.addGap(18, 18, 18)

.addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)

.addComponent(btnMaHoa)

.addComponent(btnGiaiMa))

.addContainerGap(42, Short.MAX\_VALUE))

);

pack();

}// </editor-fold>

private void btnGiaiMaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

String banma=this.txtbanma.getText();

String k = this.txtkhoa.getText();

String kt1= "";

int kn=k.length();

for(int i=0;i<kn;i++)

kt1+=(char)(((26-(Character.toUpperCase(k.charAt(i))-'A'))%26)+'A');

this.txtkhoa.setText(kt1);

String banro= mahoa(banma, kt1);

this.txtbanro.setText(banro);

}

private void btnMaHoaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

String banro = this.txtbanro.getText();

String k = this.txtkhoa.getText();

String banma= mahoa(banro, k);

this.txtbanma.setText(banma);

}

private String mahoa(String banro, String key){

int n=banro.length();

String banma= "";

int k=0;

for(int i=0; i<n; i++)

if(Character.isLetter(banro.charAt(i)))

{

banma+=mahoa(banro.charAt(i), key.charAt(k));

k++;

k=k%key.length();

}else

banma+=banro.charAt(i);

return banma;

}

char mahoa(char x, char k)

{

int xn= Character.toUpperCase(x)-'A';

int kn= Character.toUpperCase(k)-'A';

int yn= vig[kn][xn];

return (char)(yn+'A');

}

1. thuật toán Play Fair

public class class4 extends javax.swing.JFrame {

char pf[][] = {

{'M', 'O', 'N', 'A', 'R'},

{'C', 'H', 'Y', 'B', 'D'},

{'E', 'F','G', 'I', 'K'},

{'L', 'P', 'Q','S', 'T'},

{'U', 'V', 'W', 'X', 'Z'}

};

public class4() {

initComponents();

}

private void btnmahoaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

String banro= this.txtbr.getText();

banro=banro.toUpperCase();

banro=banro.replace('J','I');

String banma=mahoa(banro);

this.txtbanma.setText(banma);

}

private String mahoa(String banro){

int n=banro.length();

int i=0;

String banma="";

char a,b;

while (i<n)

{

if(i==n-1)

{

a=banro.charAt(i);

b='X';

i++;

}else{

a=banro.charAt(i);

b=banro.charAt(i+1);

if(a==b)

{

b='X';

i++;

}else

i+=2;

}

banma+=thayThe(a,b);

}

return banma;

}

String thayThe(char a, char b){

String vta=timViTri(a);

String vtb=timViTri(b);

char x, y;

if(vta.charAt(0) ==vtb.charAt(0)) //cung dong

{

x=pf[vta.charAt(0)-'0'][((vta.charAt(1)-'0')+1)%5];

y=pf[vtb.charAt(0)-'0'][((vtb.charAt(1)-'0')+1)%5];

return x+""+y;

}

if(vta.charAt(1)==vtb.charAt(1))//cung dong

{

x=pf[((vta.charAt(0)-'0')+1)%5][(vta.charAt(1)-'0')];

y=pf[((vtb.charAt(0)-'0')+1)%5][(vtb.charAt(1)-'0')];

return x+""+y;

}

x=pf[(vta.charAt(0)-'0')][(vtb.charAt(1)-'0')];

y=pf[(vtb.charAt(0)-'0')][(vta.charAt(1)-'0')];

return x+""+y;

}

private String timViTri(char a){

for(int i=0;i<5;i++)

for(int j=0;j<5;j++)

if(pf[i][j]==a)

return i+""+j;

return"";

}

private void btngiaimaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

String banma=this.txtbanma.getText();

String banro=giaima(banma);

int n = banro.length();

String br="";

for(int i=0; i<n-2;i+=2)

if(banro.charAt(i) == banro.charAt(i+2))

br +=banro.charAt(i);

else

br +=banro.charAt(i) + ""+banro.charAt(i+1);

if(banro.charAt(n-1)=='X')

br+=banro.charAt(n-2);

else

br+=banro.charAt(n-2); br+=banro.charAt(n-1);

this.txtbr.setText(br);

}

private void txtkhoaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

}

private String giaima(String banma){

int n= banma.length();

String banro="";

char a,b;

for(int i=0; i<n; i+=2){

a=banma.charAt(i);

b=banma.charAt(i+1);

banro +=thayTheNguoc(a,b);

}

return banro;

}

String thayTheNguoc(char a, char b){

String vta=timViTri(a);

String vtb=timViTri(b);

char x,y;

if(vta.charAt(0)==vtb.charAt(0))//cung dong

{

x=pf[vta.charAt(0)-'0'][((vta.charAt(1)-'0')-1)%5];

y=pf[vtb.charAt(0)-'0'][((vtb.charAt(1)-'0')-1)%5];

return x+""+y;

}

if(vta.charAt(1)==vtb.charAt(1))//cung dong

{

x=pf[((vta.charAt(0)-'0')-1+5)%5][(vta.charAt(1)-'0')];

y=pf[((vtb.charAt(0)-'0')-1+5)%5][(vtb.charAt(1)-'0')];

return x+""+y;

}

x=pf[(vta.charAt(0)-'0')][(vtb.charAt(1)-'0')];

y=pf[(vtb.charAt(0)-'0')][(vta.charAt(1)-'0')];

return x+""+y;

}

1. thuật toán DES

private int mode;

public static void doCopy(InputStream is, OutputStream os) throws IOException{

byte[] bytes = new byte[64];

int numBytes;

while((numBytes = is.read(bytes)) != -1){

os.write(bytes, 0, numBytes);

}

os.flush();

os.close();

is.close();

}

public static void encrypt(String key, InputStream is, OutputStream os) throws Throwable{

encryptOrDecrypt(key, Cipher.ENCRYPT\_MODE,is,os);

}

public static void decrypt(String key, InputStream is, OutputStream os) throws Throwable{

encryptOrDecrypt(key, Cipher.DECRYPT\_MODE,is,os);

}

public static void encryptOrDecrypt(String key, int mode,InputStream is, OutputStream os)throws Throwable{

DESKeySpec dks = new DESKeySpec(key.getBytes());

SecretKeyFactory skf = SecretKeyFactory.getInstance("DES");

SecretKey desKey= skf.generateSecret(dks);

Cipher cipher = Cipher.getInstance("DES");

if(mode == Cipher.ENCRYPT\_MODE){

cipher.init(Cipher.ENCRYPT\_MODE, desKey);

CipherInputStream cis = new CipherInputStream(is,cipher);

doCopy(cis,os);

}else if(mode == Cipher.DECRYPT\_MODE){

cipher.init(Cipher.DECRYPT\_MODE, desKey);

CipherOutputStream cos = new CipherOutputStream(os,cipher);

doCopy(is,cos);

}

}

private void btnHienthiActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

try{

BufferedReader br = null;

String fileName = "D:\\EnDes.txt";

br = new BufferedReader(new FileReader(fileName));

StringBuffer sb = new StringBuffer();

JOptionPane.showMessageDialog(null, "Da mo file!!!");

char[] ca = new char[5];

while(br.ready()){

int len = br.read(ca);

sb.append(ca, 0, len);

}

br.close();

String chuoi = sb.toString();

txtPt.setText(chuoi);

}catch(IOException ex){

Logger.getLogger(class5.class.getName()). log(Level.SEVERE, null, ex);

}

}

private void btnGhiActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

try{

BufferedWriter bw = null;

String fileName = "D:\\Des.txt";

String s = txtPt.getText();

bw = new BufferedWriter(new FileWriter(fileName));

bw.write(s);

bw.close();

JOptionPane.showMessageDialog(null, "Da ghi file!!!");

//txtCt.setText(s);

}catch(IOException ex){

Logger.getLogger(class5.class.getName()).log(Level.SEVERE, null, ex);

}

}

private void btnMahoaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

try{

String key = txtKhoa.getText();

FileInputStream fis = new FileInputStream("D:\\Des.txt");

FileOutputStream fos = new FileOutputStream("D:\\EnDes.txt");

encrypt(key, fis, fos);

JOptionPane.showMessageDialog(null, "Đã mã hóa văn bản!!");

}catch(Throwable e){

e.printStackTrace();

}

}

private void btnGiaimaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

FileInputStream fis2 = null;

try{

String key = txtKhoa.getText();

fis2 = new FileInputStream("D:\\EnDes.txt");

FileOutputStream fos2 = new FileOutputStream("D:\\DeDes.txt");

decrypt(key, fis2, fos2);

BufferedReader br = null;

br = new BufferedReader(new FileReader("D:\\DeDes.txt"));

StringBuffer sb = new StringBuffer();

JOptionPane.showMessageDialog(null, "Đã giải mã!!!");

char[] ca = new char[5];

while(br.ready()){

int len = br.read(ca);

sb.append(ca, 0, len);

}

br.close();

System.out.print(sb);

String chuoi = sb.toString();

txtPt.setText(chuoi);

}catch(Throwable ex){

Logger.getLogger(class5.class.getName()).log(Level.SEVERE, null, ex);

}finally{

try{

fis2.close();

}catch(IOException ex){

Logger.getLogger(class5.class.getName()).log(Level.SEVERE, null, ex);

}

}

}

1. thuật toán 3DES

public class FR3DES extends javax.swing.JFrame {

private static final String UNICODE\_FORMAT = "UTF8";

private static final String DESEDE\_ENCRYTION\_SCHEME = "DESede";

private KeySpec myKeySpec;

private SecretKeyFactory mySecretKeyFactory;

private Cipher cipher;

byte[] keyAsBytes;

private String myEncryptionKey;

private String myEncryptionScheme;

SecretKey key;

/\*\*

\* Creates new form FR3DES

\*/

public FR3DES() {

initComponents();

}

private void btnmahoaActionPerformed(java.awt.event.ActionEvent evt) {

try{

myEncryptionKey = txtkhoa.getText();

myEncryptionScheme = DESEDE\_ENCRYTION\_SCHEME;

keyAsBytes = myEncryptionKey.getBytes(UNICODE\_FORMAT);

myKeySpec = new DESedeKeySpec(keyAsBytes);

mySecretKeyFactory = SecretKeyFactory.getInstance(myEncryptionScheme);

cipher = Cipher.getInstance(myEncryptionScheme);

key = mySecretKeyFactory.generateSecret(myKeySpec);

System.out.println("khoa ma hoa la:"+ "" + key);

String plaintText =txtplaintext.getText();

String encrypted=encrypt(plaintText);

System.out.println("Encrypted Value"+ encrypted);

txtciphertext.setText(encrypted);

}catch(Exception e){

System.out.println("Loi ma hoa"+ e);

}

// TODO add your handling code here:

}

private void btnhienthiActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

try{

BufferedReader br = null;

String fileName ="E:\\GhiDESEDE.txt";

br = new BufferedReader(new FileReader(fileName));

StringBuffer sb = new StringBuffer();

JOptionPane.showMessageDialog(null," da mo file");

char[] ca = new char[5];

while(br.ready()){

int len = br.read(ca);

sb.append(ca,0,len);

}

br.close();

System.out.println("Du lieu la:"+ " "+ sb);

String chuoi = sb.toString();

txtplaintext.setText(chuoi);

btngiaima.enable(true);

}catch(Exception ex)

{

Logger.getLogger(FR3DES.class.getName()).log(Level.SEVERE, null,ex);

}

}

private void btnghifileActionPerformed(java.awt.event.ActionEvent evt) {

try{

BufferedWriter bw = null;

String fileName ="E:\\GhiDESEDE.txt";

String s= txtciphertext.getText();

bw = new BufferedWriter(new FileWriter(fileName));

bw.write(s);

bw.close();

JOptionPane.showMessageDialog(null, "Da ghi file");

}catch(Exception ex)

{

Logger.getLogger(FR3DES.class.getName()).log(Level.SEVERE, null,ex);

}

// TODO add your handling code here:

}

private void btngiaimaActionPerformed(java.awt.event.ActionEvent evt) {

}

private void btnallshowActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

}

public String encrypt(String unencryptedString) {

String encryptedString = null;

try {

cipher.init(Cipher.ENCRYPT\_MODE, key);

byte[] plainText = unencryptedString.getBytes(UNICODE\_FORMAT);

byte[] encryptedText = cipher.doFinal(plainText);

BASE64Encoder base64encoder= new BASE64Encoder();

encryptedString = base64encoder.encode(encryptedText);

} catch (Exception e) {

e.printStackTrace();

}

return encryptedString;

}

public String decrypt(String encryptedString) {

String decryptedText=null;

try {

cipher.init(Cipher.DECRYPT\_MODE, key);

BASE64Decoder base64encoder= new BASE64Decoder();

byte[] encryptedText = base64encoder.decodeBuffer(encryptedString);

byte[] plainText = cipher.doFinal(encryptedText);

decryptedText= new String(plainText);

} catch (Exception e) {

e.printStackTrace();

}

return decryptedText;

}

1. thuật toán RAILFENCE

private void mahoabtnActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

int k=Integer.valueOf(this.txtKhoa.getText());

String s= this.txtbr.getText();

int n=s.length();

int sd, sc;

sd=k;

sc= n/sd+1;

char hr[][]= new char[sd][sc];

int c,d;

c=0;d=0;

int sodu = n%sd;

for(int i = 0;i<n; i++)

{

hr[d][c]= s.charAt(i);

d++;

if(d==k)

{

c++; d=0;

}

}

String kq="";

int sokytu=sc;

for(int i=0;i<sd;i++)

{

if(i >=sodu) sokytu=sc-1;

for (int j=0; j<sokytu; j++)

kq=kq+hr[i][j];

}

this.txtbm.setText(kq);

}

private void jButton2ActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

String cipherText = txtbm.getText();

int r = Integer.parseInt(txtKhoa.getText());//khóa củng là số dòng

String result = "";

int s;//số cột của mảng

if (cipherText.length() % r == 0) {

s = cipherText.length() / r;

} else {

s = (cipherText.length() / r) + 1;

}

for (int i = 0; i < s; i++) {

int k = i;

while (k < cipherText.length()) {

result += cipherText.charAt(k);

k+=(r+1);

}

}

// int k = 0;

// char ct[][] = new char[r][s];

// for (int i = 0; i < r; i++) {

// for (int j = 0; j < s; j++) {

// if (k >= cipherText.length()) {

// break;

// }

// ct[i][j] = cipherText.charAt(k);

// k++;

// }

// }

//

// for (int i = 0; i < s; i++) {

// for (int j = 0; j < r; j++) {

// if (ct[j][i] == 0) {

// result += '\0';

// } else {

// result += ct[j][i];

// }

// }

// }

//

// String s1 = "";

// for (k = 0; k < result.length(); k++) {

// if (((int) result.charAt(k)) != 0) {

// s1 += result.charAt(k);

// }

// }

txtbr.setText(result);

}

1. thuật toán AES.

public class AES extends javax.swing.JFrame {

public AES() {

initComponents();

}

private void btndangnhapActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here

try{

user= txtuser.getText();

pass= txtpas.getText();

xacthuc = user +pass;

BufferedReader br = null;

String fileName ="E:\\AES.txt";

br = new BufferedReader(new FileReader(fileName));

StringBuffer sb= new StringBuffer();

char[] ca = new char[5];

while (br.ready()) {

int len=br.read(ca);

sb.append(ca,0,len);

}

br.close();

System.out.println("Khoa la:"+ ""+ sb);

String chuoi = sb.toString();

Boolean k =xacthuc.equals(chuoi);

if(k==true){

JOptionPane.showMessageDialog(null,"Đăng nhập thành công");

}else

JOptionPane.showMessageDialog(null,"Đăng nhập thất bại");

txtmadk.setText(chuoi.getBytes().toString());

KeyGenerator KeyGen = KeyGenerator.getInstance("AES");

KeyGen.init(128);

secretKey = KeyGen.generateKey();

}catch(NoSuchAlgorithmException ex){

}catch(Exception ex){

}

}

private void btndangkyActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

try{

user= txtuser.getText();

pass= txtpas.getText();

xacthuc = user +pass;

BufferedWriter bw = null;

String fileName = "E:\\AES.txt";

String s= txtplaintext.getText();

bw=new BufferedWriter (new FileWriter(fileName));

bw.write(xacthuc);

bw.close();

JOptionPane.showMessageDialog(null, "Đăng ký thàng công");

txtmadk.setText(xacthuc.getBytes().toString());

}catch(Exception ex){

Logger.getLogger(AES.class.getName()).log(Level.SEVERE,null,ex);

}

}

private void btnmahoaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

try{

System.out.println("Sinh khoa"+ secretKey);

Cipher aesCipher = Cipher.getInstance("AES");

aesCipher.init(Cipher.ENCRYPT\_MODE, secretKey);

String strData = txtplaintext.getText();

byte[] byteDataToEncrypt = strData.getBytes();

byteCipherText = aesCipher.doFinal(byteDataToEncrypt);

String strCipherText = new BASE64Encoder().encode(byteCipherText);

System.out.println("Cipher Text generated using AES is" + strCipherText);

txtcipher.setText(strCipherText);

}catch(Exception ex)

{

System.out.println("Loi ma hoa"+ ex);

}

}

private void btngiaimaActionPerformed(java.awt.event.ActionEvent evt) {

try{

String cipherText=txtcipher.getText();

txtplaintext.setText(cipherText);

Cipher aesCipher = Cipher.getInstance("AES");

aesCipher.init(Cipher.DECRYPT\_MODE, secretKey,aesCipher.getParameters());

byte[] byteDecryptedText= aesCipher.doFinal(byteCipherText);

String strDecryptedText = new String(byteDecryptedText);

System.out.println("Decrypted Text massage is"+ strDecryptedText);

txtcipher.setText(strDecryptedText);

}catch(Exception ex)

{

System.out.println("Loi giai ma"+ ex);

}

// TODO add your handling code here:

}

private void btnghifileActionPerformed(java.awt.event.ActionEvent evt) {

try{

BufferedWriter bw = null;

String fileName ="E:\\GhiAES.txt";

String s= txtcipher.getText();

bw = new BufferedWriter(new FileWriter(fileName));

bw.write(s);

bw.close();

JOptionPane.showMessageDialog(null, "Da ghi file");

}catch(Exception ex)

{

Logger.getLogger(AES.class.getName()).log(Level.SEVERE, null,ex);

}

// TODO add your handling code here:

}

private void btnmofileActionPerformed(java.awt.event.ActionEvent evt) {

try{

BufferedReader br = null;

String fileName ="E:\\GhiAES.txt";

br = new BufferedReader(new FileReader(fileName));

StringBuffer sb = new StringBuffer();

JOptionPane.showMessageDialog(null," da mo file");

char[] ca = new char[5];

while(br.ready()){

int len = br.read(ca);

sb.append(ca,0,len);

}

br.close();

System.out.println("Du lieu la:"+ " "+ sb);

String chuoi = sb.toString();

txtplaintext.setText(chuoi);

btngiaima.enable(true);

}catch(Exception ex)

{

Logger.getLogger(AES.class.getName()).log(Level.SEVERE, null,ex);

}

// TODO add your handling code here:

}

1. RSA(Form)\*

RSA rsa = new RSA(8);

BigInteger[] ciphertext = null;

BigInteger n= null;

BigInteger d= null;

String message;

/\*\*

\* Creates new form fRSA

\*/

public fRSA() {

initComponents();

}

private void btnMahoaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

String plainText = txtPt.getText();

System.out.println("van ban can ma hoa"+plainText);

n=rsa.getN();

d=rsa.getD();

ciphertext = rsa.encrypt(plainText);

StringBuilder bf = new StringBuilder();

for(int i=0; i < ciphertext.length;i++ )

{

bf.append(ciphertext[i].toString(16).toUpperCase());

if(i!=ciphertext.length - 1)

System.out.print("");

}

message=bf.toString();

System.out.println("CipherText:"+ message);

txtCt.setText(message);

}

private void btnGiaimaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

txtCt.setText(message);

String dhash = rsa.decrypt(ciphertext, d, n);

System.out.println("van ban goc la" +dhash);

txtCt.setText(dhash);

}

1. thuật toán RSA(nhức đầu).

public class class7 extends javax.swing.JFrame {

RSA rsa = new RSA(8);

BigInteger[] ciphertext = null;

BigInteger n= null;

BigInteger d= null;

String message;

/\*\*

\* Creates new form class7

\*/

public class7() {

initComponents();

}

private void btnMahoaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

String pw = txtpassword.getText();

Pattern p = Pattern.compile("[^A-Za-z0-9]");

Matcher m = p.matcher(pw);

boolean b = m.find();

if(b){

String plainText = txthoten.getText()+ "\n" + txtdiachi.getText()+"\n"+ txtemail.getText()+"\n"+ txtsdt.getText()+"\n"+ txtpassword.getText();

System.out.println("Thong tin da nhap:");

n=rsa.getN();

d=rsa.getD();

ciphertext = rsa.encrypt(plainText);

StringBuilder bf = new StringBuilder();

for(int i=0; i < ciphertext.length;i++ )

{

bf.append(ciphertext[i].toString(16).toUpperCase());

if(i!=ciphertext.length - 1)

System.out.print("");

}

message=bf.toString();

System.out.println("CipherText:"+ message);

txtmahoa.setText(message);

}

else

JOptionPane.showMessageDialog(null, "Mật khẩu phải có ki tự đặc biệt");

}

private void btnGiaimaActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

txtmahoa.setText(message);

String dhash = rsa.decrypt(ciphertext, d, n);

System.out.println("van ban goc la:" +dhash);

txtmahoa.setText(dhash);

}

private void txthotenActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

}

private void txtdiachiActionPerformed(java.awt.event.ActionEvent evt) {

// TODO add your handling code here:

}

}

1. Thuật toán SHA.

public class SHA extends javax.swing.JFrame {

/\*\*

\* Creates new form SHA

\*/

public SHA() {

initComponents();

}

private void btnbamActionPerformed(java.awt.event.ActionEvent evt) {

try{

String chuoi ="";

chuoi= txtnhapchuoi.getText();

MessageDigest md = MessageDigest.getInstance("SHA-256");

md.update(chuoi.getBytes());

byte byteData[] = md.digest();

StringBuffer sb = new StringBuffer();

for( int i=0;i<byteData.length;i++){

sb.append(Integer.toString((byteData[i] & 0xff) + 0x100, 16).substring(1));

}

System.out.println("Hex format1 : "+ sb.toString());

txtc1.setText(sb.toString());

//c2

StringBuffer hexString = new StringBuffer();

for( int i=0;i<byteData.length;i++){

String hex= Integer.toHexString(0xff & byteData[i]);

if(hex.length()==1) hexString.append('0');

hexString.append(hex);

}

System.out.println("Hex format2 : "+ hexString.toString());

txtc2.setText(hexString.toString());

}catch(NoSuchAlgorithmException ex){

Logger.getLogger(SHA.class.getName()).log(Level.SEVERE, null,ex);

}

1. Thuật toán HASH MD5.

public class HASHMD5 extends javax.swing.JFrame {

public HASHMD5() {

initComponents();

}

private void btndangkky ActionPerformed(java.awt.event.ActionEvent evt) {

try{

String user = txtusername.getText();

String pass = txtpass.getText();

String bam ="";

bam = user + pass;

MessageDigest md = MessageDigest.getInstance("MD5");

md.update(bam.getBytes());

byte[] byteData = md.digest();

StringBuffer sb = new StringBuffer();

for(int i=0;i<byteData.length;i++){

sb.append(Integer.toString((byteData[i] & 0xff) + 0x100,16).substring(1));

}

System.out.println("Digest( in hex format)::"+ sb.toString());

txtresult1.setText(sb.toString());

StringBuffer hexString = new StringBuffer();

for (int i=0;i<byteData.length; i++){

String hex= Integer.toHexString(0xff & byteData[i]);

if(hex.length()==1){

hexString.append('0');

}

hexString.append(hex);

}

System.out.println("Digest( in hex format)::"+ hexString.toString());

txtresult2.setText(hexString.toString());

txtchuoi.setText(bam.toString());

BufferedWriter bw = null;

String fileName="E:\\BamMD5.txt";

bw = new BufferedWriter(new FileWriter(fileName));

bw.write(hexString.toString());

bw.close();

JOptionPane.showMessageDialog(null, " ban da dang ky thanh cong,vui long dang nhap lai");

// TODO add your handling code here:

}

catch(Exception ex){

System.out.println("loi bam user va pass:"+ ex);}

}

private void btndangnhap ActionPerformed(java.awt.event.ActionEvent evt) {

String user = txtusername.getText();

String pass = txtpass.getText();

String bam ="";

bam = user + pass;

BufferedReader br = null;

String fileName="E:\\BamMD5.txt";

try{

br = new BufferedReader(new FileReader(fileName));

StringBuffer sb = new StringBuffer();

char[] ca = new char[5];

while (br.ready()) {

int len=br.read(ca);

sb.append(ca,0,len);

}

br.close();

System.out.println("chung thuc"+""+sb);

String chuoi = sb.toString();

MessageDigest md = MessageDigest.getInstance("MD5");

md.update(bam.getBytes());

byte[] byteData = md.digest();

StringBuffer hexString = new StringBuffer();

for(int i=0; i<byteData.length;i++){

String hex = Integer.toHexString(0xff & byteData[i]);

if(hex.length()==1){

hexString.append('0');

}

hexString.append(hex);

}

System.out.println("Bam user va pass:"+""+ hexString.toString());

Boolean k=hexString.toString().equals(chuoi);

if(k==true)

{

JOptionPane.showMessageDialog(null, " dang nhap thanh cong");

txtresult1.setText(hexString.toString());

txtresult2.setText(chuoi);

txtchuoi.setText("Username:"+user+" "+"Password: "+ pass);

} else

JOptionPane.showMessageDialog(null,"Đăng nhập thất bại");

}catch(Exception ex){

System.out.println("loi Dang Nhap"+ ex);

}

1. File code Thuật toán RSA nâng cao(code java).
2. Skey\_RSA.

public class Skey\_RSA {

public static void main(String[] args) throws Exception {

KeyPairGenerator kpg= KeyPairGenerator.getInstance("RSA");

kpg.initialize(1024);

KeyPair kp = kpg.genKeyPair();

PublicKey pbKey=kp.getPublic();

PrivateKey prKey=kp.getPrivate();

FileOutputStream f1= new FileOutputStream("E:\\Skey\_RSA\_pub.dat");

ObjectOutputStream b1= new ObjectOutputStream(f1);

b1.writeObject(pbKey);

FileOutputStream f2= new FileOutputStream("E:\\Skey\_RSA\_priv.dat");

ObjectOutputStream b2= new ObjectOutputStream(f2);

b2.writeObject(prKey);

}

}

1. ENC\_RSA.

public class Enc\_RSA {

public static void main(String[] args) throws Exception{

String s ="Hello World!";

FileInputStream f = new FileInputStream("E:\\Skey\_RSA\_pub.dat");

ObjectInputStream b = new ObjectInputStream(f);

RSAPublicKey pbk =(RSAPublicKey)b.readObject();

BigInteger e = pbk.getPublicExponent();

BigInteger n = pbk.getModulus();

System.out.println("e="+e);

System.out.println("n="+n);

byte ptext[]=s.getBytes("UTF8");

BigInteger m = new BigInteger(ptext);

BigInteger c=m.modPow(e, n);

System.out.println("c= "+c);

String cs=c.toString();

BufferedWriter out =

new BufferedWriter(new OutputStreamWriter(

new FileOutputStream("E:\\Enc\_RSA.dat")));

out.write(cs,0,cs.length());

out.close();

}

}

1. DEC\_RSA.

public class Dec\_RSA {

public static void main(String[] args) throws Exception{

BufferedReader in =

new BufferedReader(new InputStreamReader

(new FileInputStream("E:\\Enc\_RSA.dat")));

String ctext=in.readLine();

BigInteger c = new BigInteger(ctext);

FileInputStream f = new FileInputStream("E:\\Skey\_RSA\_priv.dat");

ObjectInputStream b = new ObjectInputStream(f);

RSAPrivateKey prk=(RSAPrivateKey)b.readObject();

BigInteger d=prk.getPrivateExponent();

BigInteger n=prk.getModulus();

System.out.println("d="+d);

System.out.println("n="+n);

BigInteger m=c.modPow(d, n);

System.out.println("m="+m);

byte[] mt=m.toByteArray();

System.out.println("PlainText is ");

for(int i=0;i<mt.length;i++){

System.out.print((char) mt[i]);

}

}

}