INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

“Affine Cipher”

Abstact

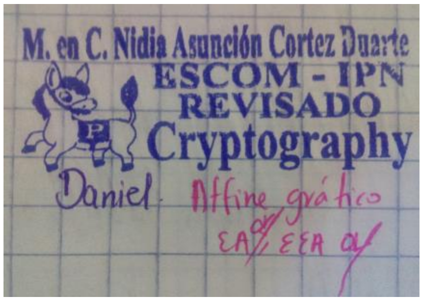
In this report I will mention about the Affine Cipher which is an encryption algorithm, also mention will be made of Euclides' extended algorithm.

By:

Meza Martínez Luis Daniel

Professor:
MSc. NIDIA ASUNCIÓN CORTEZ DUARTE

March 2018



M. en C. Nidia Asunción Cortez Duarte
ESCOM - IPN
REVISADO
Cryptography
Daniel Affine gráfico
EA ~~ok~~ EEA ok

Index

Contenido

Introduction:..1

Literature review:.....................................1

Software (libraries, packages, tools):.....................2

Procedure:..3

Results...3

Discussion:...3

Conclusions:..5

References:...5

Code..5

Introduction:

Cryptograpy is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructiong and analyzing protocols that prevent third parties of the public from reading private messages. Various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Literature review:

The affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to it´s numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. The formula used means that each letter encrypts to one other letter, and back again, meaning the cipher is essentially a standard substitution cipher with a rule governing which letter goes to which. As such, it has the weaknesses of all substitution ciphers. Each letter is enciphered with the function $(\alpha x + \beta) \, mod \, 26$, where β is the magnitude of the shift.You should include diagrams, formulas, algortithms.

In the affine cipher the letters of an alphabet of size m are first mapped to the integers in the range $0 \dots m - 1$. It then uses modular arithmetic to transform the integer that each plaintext letter corresponds to into another integer that correspond to a ciphertext letter. The encryption function for a single letter is:

$$E(x) \; = (\alpha x + \beta) mod \; m$$

Where modulus m is the size of the alphabet and α and β are the key of the cipher.

The decription function is:

$$D(x) \; = \propto^{-1} (x + (-\beta)) mod \; m$$

Where $\propto^{-1}$ is the multiplicative inverse of α. And $-\beta$ is the additive inverse.

To calculate the inverse multiplicative we use the euclidean algorithm extended.

In arithmetic and computer programming, the extended Euclidean algorithm is an extension to the Euclidean algorithm, and computes, in addition to the greatest common divisor of integers a and b, also the coefficients of Bézout's identity, which are integers x and y such that

$$ax + by = \gcd(a, b)$$

The extended Euclidean algorithm is particularly useful when a and b are coprime, since x is the modular multiplicative inverse of a modulo b, and y is the modular multiplicative inverse of b modulo a. Similarly, the polynomial extended Euclidean algorithm allows one to compute the multiplicative inverse in algebraic field extensions and, in particular in finite fields of non prime order. It follows that both extended Euclidean algorithms are widely used in cryptography. In particular, the computation of the modular multiplicative inverse is an essential step in RSA public-key encryption method.

Software (libraries, packages, tools):

In the lab the only things I use to learn about to make the gcd was the book of "matemáticas discretas" and check the notes I made in the class.

For the realization of this practice the language that I used to carry out this practice was Java, and the IDE that I use netbeans, because I needed a graphic interface and it was easier for me to develop in netbeans.

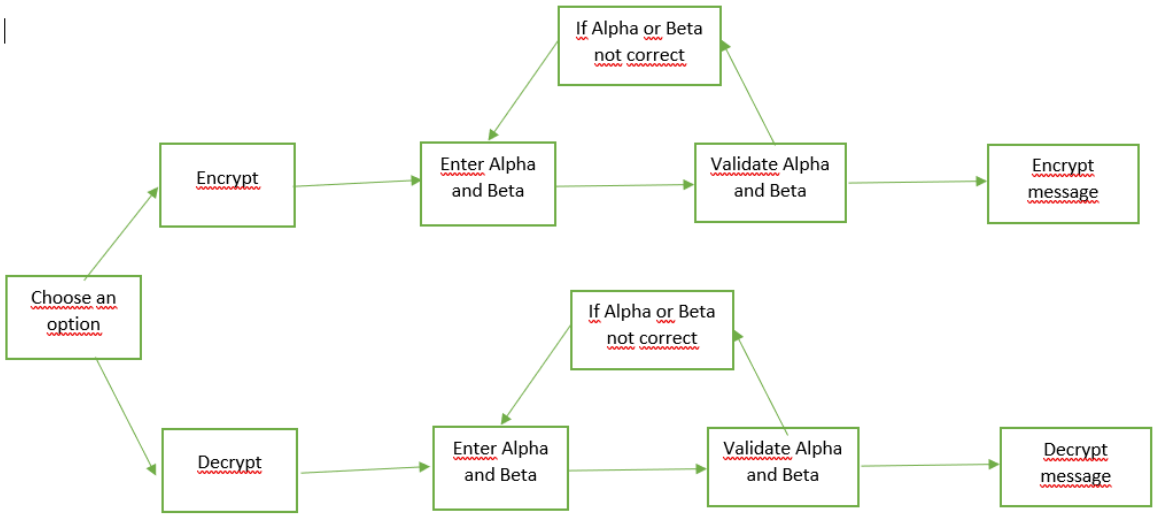
First, I did the program in C, because I like to program in C because I like much easier to work at a bit level, and I think that if I can program it in C, doing it in another programming language will be easy.

I thought to present this practice in python, however I still need to study the graphic part of python, in the future I hope to have a better graphic interface.

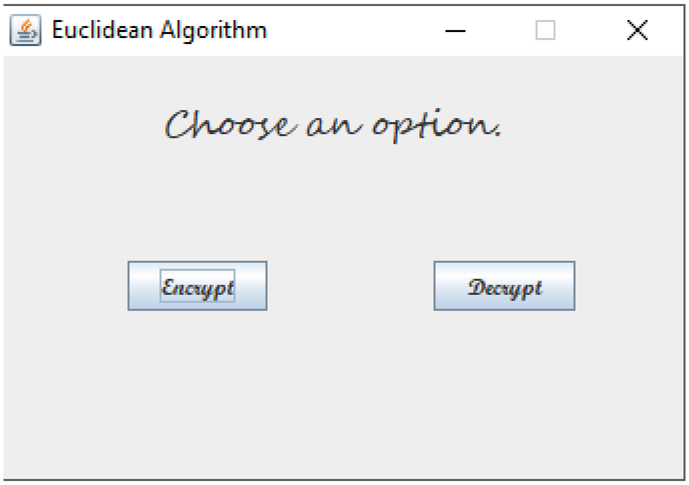
The package I use to make the functions in NetBeans:

```
import java.io.BufferedReader;
import java.io.File;
import java.io.FileNotFoundException;
import java.io.FileReader;
import java.io.FileWriter;
import java.io.PrintWriter;
import java.util.logging.Level;
import java.util.logging.Logger;
import javax.swing.JFileChooser;
```

Procedure:



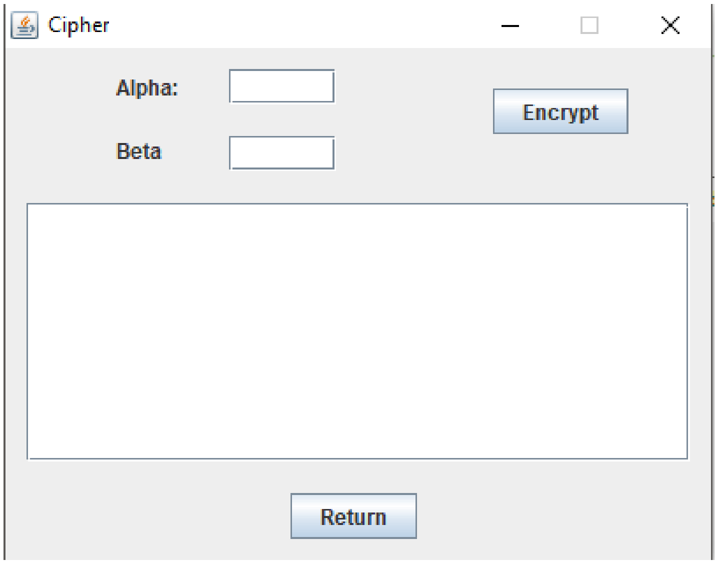
Results


Euclidean Algorithm

Choose an option.

First we see the interface and choose an option, in this case we choose Encrypt

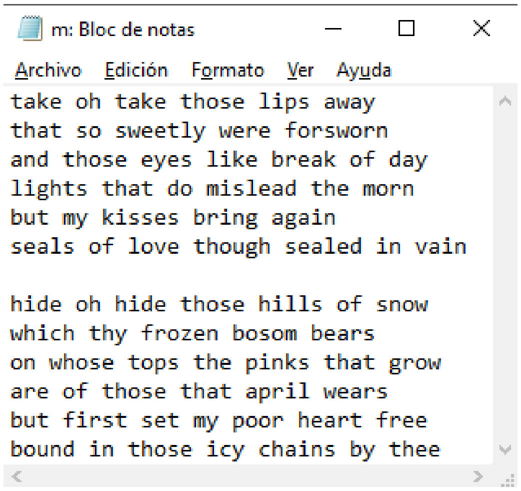
Now we need to write an Alpha and Beta, remember; Alpha does not accept even numbers or multiples of 13, beta must be greater than 0 and less than 27.


Cipher

Alpha:

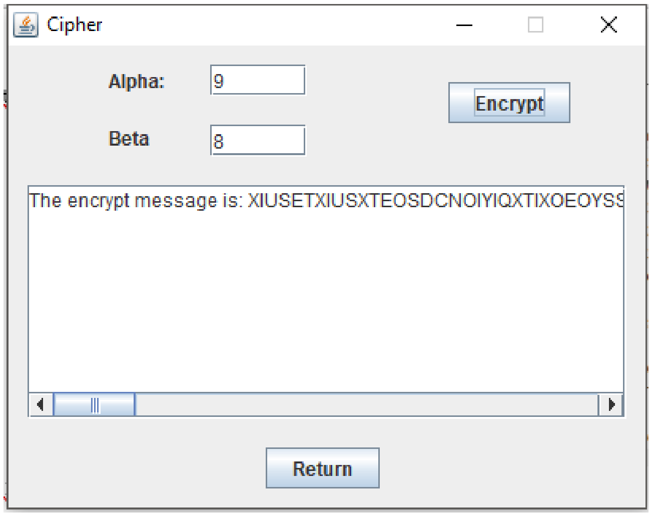
Beta

The message that exists in the m.txt file is



```
take oh take those lips away
that so sweetly were forsworn
and those eyes like break of day
lights that do mislead the morn
but my kisses bring again
seals of love though sealed in vain

hide oh hide those hills of snow
which thy frozen bosom bears
on whose tops the pinks that grow
are of those that april wears
but first set my poor heart free
bound in those icy chains by thee
```



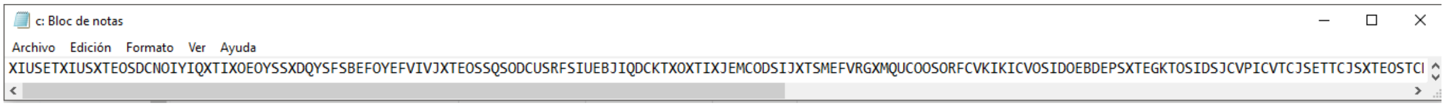
Alpha: 9

Beta 8

The encrypt message is: XIUSETXIUSXTEOSDCNOIYIQXTIXOEOYSS

For example, we put in Alpha 9 and in beta 8

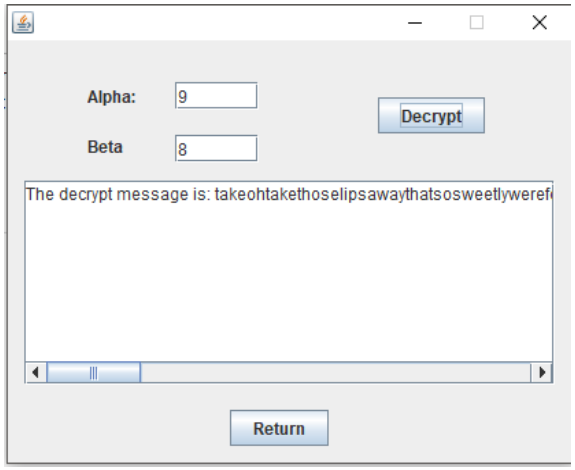
In the screen we can be the encrypt message, and we can found the encrypted message in our carpet in an archive with the nambe c.txt



```
XIUSETXIUSXTEOSDCNOIYIQXTIXOEOYSSXDQYSFSBEFOYEFVIVJXTEOSSQSODCUSRFSIUEBJIQDCKTXOXTIXJEMCODSIJXTSMEFVRGXMQUCOOSORFCVKIKICVOSIDOEBDEPSXTEGKTOSIDSJCVPICVTCJSETTCJSXTEOSTC
```

If we see the archive, the message was encrypted.

If we try to decrypt the message we need top ut an Alpha and beta, must match the alpha and beta introduced in the encryption if we put a different alpha and beta to the one that we enter our message will not be decrypted correctly, and will generate a different decrypted file.

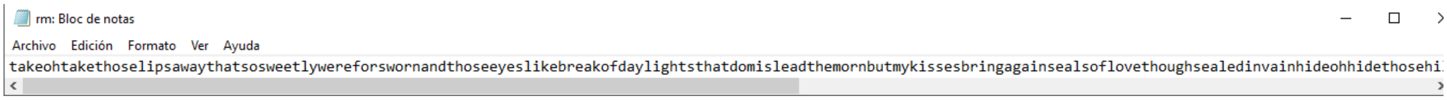


Alpha: 9

Beta 8

The decrypt message is: takeohtakethoselipsawaythatsosweetlyweref

If we put the correct Alpha and beta we can see the decrypt message whitouth spaces.



```
takeohtakethoselipsawaythatsosweetlywereforswornandthoseeyeslikebreakofdaylightsthatdomisleadthemornbutmykissesbringagainsealsoflovethoughsealedinvainhideohhidethosehi
```

In the archive rm.txt we can see the decrypt message.

Discussion:

In comparison with what was seen in the classroom, the practice had a medium degree of complexity, since we had to generate the functions to validate Alpha and beta, and it was not as simple as we did in class, since we use the extended Euclid algorithm, which is very useful for the realization of this practice

Conclusions:

In this practice I had to remember some things in Java, because I almost do not plan to use a graphical interface, and I prefer the use of a console, however it was not so difficult to implement, I had to investigate many things on my own and it was a practice that I liked a lot because of the complexity level of the Euclide's algorithm.

References:

Johnsonbaugh, R. and González Osuna, M. (2005). *Matemáticas discretas*. México: Pearson Educación.

Code

Main:

```java
package prc4;
import java.util.Scanner;
public class Prc4
{
    public static void main(String[] args)
    {
        int alpha=0, beta=0;
        System.out.println("Euclidean algorithm");
        new EuclideanAlgorithm().setVisible(true);
        new Cipher().setVisible(false);
        new Decipher().setVisible(false);
    }
}
```

Cipher

```java
package prc4;

import java.io.BufferedReader;
    import java.io.File;
    import java.io.FileNotFoundException;
    import java.io.FileReader;
    import java.io.FileWriter;
    import java.io.PrintWriter;
    import java.util.logging.Level;
    import java.util.logging.Logger;
    import javax.swing.JFileChooser;

public class Cipher extends javax.swing.JFrame {
    int alpha=0, beta=0;
    public Cipher()
    {
        initComponents();
        this.setLocationRelativeTo(null);

    }

    @SuppressWarnings("unchecked")
    // <editor-fold defaultstate="collapsed" desc="Generated Code">
    private void initComponents() {

        jScrollPane1 = new javax.swing.JScrollPane();
        TextCipher = new javax.swing.JTextArea();
        ReturnButton = new javax.swing.JButton();
        jLabel1 = new javax.swing.JLabel();
        jLabel2 = new javax.swing.JLabel();
        EntAlpha = new javax.swing.JTextField();
        EntBeta = new javax.swing.JTextField();
        Crypt = new javax.swing.JButton();

        setDefaultCloseOperation(javax.swing.WindowConstants.EXIT_ON_CLOSE);
        setTitle("Cipher");
        setResizable(false);

        TextCipher.setColumns(20);
        TextCipher.setRows(5);
        jScrollPane1.setViewportView(TextCipher);

        ReturnButton.setText("Return");
        ReturnButton.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                ReturnButtonActionPerformed(evt);
            }
        });

        jLabel1.setText("Alpha:");

        jLabel2.setText("Beta");

        EntAlpha.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                EntAlphaActionPerformed(evt);
            }
        });

        EntBeta.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                EntBetaActionPerformed(evt);
            }
        });

        Crypt.setText("Encrypt");
        Crypt.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                CryptActionPerformed(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()
                .addComponent(jScrollPane1)
                .addContainerGap())
            .addGroup(layout.createSequentialGroup()
                .addGap(63, 63, 63)
                .addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
                    .addComponent(jLabel1)
                    .addComponent(jLabel2))
                .addGap(29, 29, 29)
                .addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING, false)
                    .addComponent(EntAlpha, javax.swing.GroupLayout.DEFAULT_SIZE, 61, Short.MAX_VALUE)
                    .addComponent(EntBeta))
                .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED, 89, Short.MAX_VALUE)
                .addComponent(Crypt)
                .addGap(47, 47, 47))
            .addGroup(layout.createSequentialGroup()
                .addGap(162, 162, 162)
                .addComponent(ReturnButton)
                .addContainerGap(javax.swing.GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE))
        );
        layout.setVerticalGroup(
            layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
                  .addGroup(layout.createSequentialGroup()
                      .addContainerGap()
                      .addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
                          .addGroup(layout.createSequentialGroup()
                              .addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.BASELINE)
                                  .addComponent(jLabel1)
                                  .addComponent(EntAlpha, javax.swing.GroupLayout.PREFERRED_SIZE, javax.swing.GroupLayout.DEFAULT_SIZE, javax.swing.GroupLayout.PREFERRED_SIZE))
                              .addGap(18, 18, 18))
                          .addGroup(javax.swing.GroupLayout.Alignment.TRAILING, layout.createSequentialGroup()
                              .addComponent(Crypt)
                              .addGap(1, 1, 1)))
                      .addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
                          .addComponent(jLabel2)
                          .addComponent(EntBeta, javax.swing.GroupLayout.PREFERRED_SIZE, 20, javax.swing.GroupLayout.PREFERRED_SIZE))
                      .addGap(18, 18, 18)
                      .addComponent(jScrollPane1, javax.swing.GroupLayout.DEFAULT_SIZE, 147, Short.MAX_VALUE)
                      .addGap(18, 18, 18)
                      .addComponent(ReturnButton)
                      .addContainerGap())
              );

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

```

```
    private void ReturnButtonActionPerformed(java.awt.event.ActionEvent evt) {
        new EuclideanAlgorithm().setVisible(true);
       //Cierra la ventana actual
       dispose();
    }

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

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

    private void CryptActionPerformed(java.awt.event.ActionEvent evt) {
        if(EntAlpha.getText().length() == 0 || EntBeta.getText().length()==0)
        {
            TextCipher.setText("Please enter the value of alpha and beta");
            EntAlpha.setText(null);
            EntBeta.setText(null);
        }
        else
        {
            alpha = Integer.parseInt(EntAlpha.getText());
            beta = Integer.parseInt(EntBeta.getText());
            if(alpha%2==0 || alpha%13==0 || alpha < 0 || alpha>25 || beta<1 || beta>26)
            {
                TextCipher.setText("Wrong this value cannot be accepted");
                EntAlpha.setText(null);
                EntBeta.setText(null);
            }
            else
            {
                char caracter, caracter1, nuevPal, c, newLet;
                String mensaje = "", msjPant="";
                int car, n;
                FileReader fr = null;
                FileWriter fw = null;
                PrintWriter pw = null;
                try
                {
                    fr = new FileReader ("C:\\Users\\Daniel\\Desktop\\ESCOM\\7mo semestre\\Cryptography\\Prc4\\m.txt");
                    fw = new FileWriter("C:\\Users\\Daniel\\Desktop\\ESCOM\\7mo semestre\\Cryptography\\Prc4\\c.txt");
                    pw = new PrintWriter(fw);
                    car = fr.read();
                    while(car != -1)
                    {
                        //TextCipher.setText(car);
                        if(car==32|| car==10 ||car==13)
                        {
                            car = fr.read();
                        }
                        else
                        {
                            nuevPal = (char) (car - 97);
                            c = (char) ((nuevPal*alpha +beta)%26);
                            newLet = (char) (c + 65);
                            mensaje = mensaje+String.valueOf(newLet);
```

```
                                   car = fr.read();
                               }

                           }
                           msjPant +=mensaje;
                           System.out.println(msjPant);
                           TextCipher.setText("The encrypt message is: "+ msjPant);
                           System.out.println("Alpha:"+alpha+" Beta: "+beta);

                           pw.println(mensaje);
                           fw.close();
                           fr.close();

                      }
                      catch(Exception 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(Cipher.class.getName()).log(java.util.logging.Level.SEVERE, null, ex);
               } catch (InstantiationException ex) {
                   java.util.logging.Logger.getLogger(Cipher.class.getName()).log(java.util.logging.Level.SEVERE, null, ex);
               } catch (IllegalAccessException ex) {
                   java.util.logging.Logger.getLogger(Cipher.class.getName()).log(java.util.logging.Level.SEVERE, null, ex);
               } catch (javax.swing.UnsupportedLookAndFeelException ex) {
                   java.util.logging.Logger.getLogger(Cipher.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 Cipher().setVisible(true);
                   }
               });
```

```
        }

        // Variables declaration - do not modify
        private javax.swing.JButton Crypt;
        private javax.swing.JTextField EntAlpha;
        private javax.swing.JTextField EntBeta;
        private javax.swing.JButton ReturnButton;
        private javax.swing.JTextArea TextCipher;
        private javax.swing.JLabel jLabel1;
        private javax.swing.JLabel jLabel2;
        private javax.swing.JScrollPane jScrollPane1;
        // End of variables declaration
    }
```

Decipher

```
package prc4;

import java.io.FileReader;
import java.io.FileWriter;
import java.io.IOException;
import java.io.PrintWriter;

public class Decipher extends javax.swing.JFrame {

    public Decipher() {
        initComponents();
        this.setLocationRelativeTo(null);
    }

    @SuppressWarnings("unchecked")
    // <editor-fold defaultstate="collapsed" desc="Generated Code">
    private void initComponents() {

        jLabel1 = new javax.swing.JLabel();
        EntAlpha = new javax.swing.JTextField();
        jLabel2 = new javax.swing.JLabel();
        EntBeta = new javax.swing.JTextField();
        Decipher = new javax.swing.JButton();
        jScrollPane1 = new javax.swing.JScrollPane();
        TextCipher = new javax.swing.JTextArea();
        ReturnButton = new javax.swing.JButton();

        setDefaultCloseOperation(javax.swing.WindowConstants.EXIT_ON_CLOSE);
        setResizable(false);

        jLabel1.setText("Alpha:");

        EntAlpha.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                EntAlphaActionPerformed(evt);
            }
        });

        jLabel2.setText("Beta");

        EntBeta.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                EntBetaActionPerformed(evt);
            }
        });

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

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

        TextCipher.setColumns(20);
        TextCipher.setRows(5);
        jScrollPane1.setViewportView(TextCipher);

        ReturnButton.setText("Return");
        ReturnButton.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                ReturnButtonActionPerformed(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()
                .addGap(58, 58, 58)
                .addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
                    .addComponent(jLabel1)
                    .addComponent(jLabel2))
                .addGap(29, 29, 29)
                .addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING, false)
                    .addComponent(EntAlpha)
                    .addComponent(EntBeta, javax.swing.GroupLayout.PREFERRED_SIZE, 61, javax.swing.GroupLayout.PREFERRED_SIZE))
                .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED, 87, Short.MAX_VALUE)
                .addComponent(Decipher)
                .addGap(63, 63, 63))
            .addGroup(layout.createSequentialGroup()
                .addGap(162, 162, 162)
                .addComponent(ReturnButton)
                .addContainerGap(javax.swing.GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE))
            .addGroup(javax.swing.GroupLayout.Alignment.TRAILING, layout.createSequentialGroup()
                .addContainerGap()
                .addComponent(jScrollPane1)
                .addContainerGap())
        );
        layout.setVerticalGroup(
            layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addGroup(layout.createSequentialGroup()
                .addGap(30, 30, 30)
                .addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
                    .addGroup(layout.createSequentialGroup()
                        .addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.BASELINE)
                            .addComponent(jLabel1)
                            .addComponent(EntAlpha, javax.swing.GroupLayout.PREFERRED_SIZE, javax.swing.GroupLayout.DEFAULT_SIZE, javax.swing.GroupLayout.PREFERRED_SIZE))
                        .addGap(18, 18, 18))
                          .addGroup(javax.swing.GroupLayout.Alignment.TRAILING, layout.createSequentialGroup()
                              .addComponent(Decipher)
                              .addGap(1, 1, 1)))
                      .addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
                          .addComponent(jLabel2)
                          .addComponent(EntBeta, javax.swing.GroupLayout.PREFERRED_SIZE, 20, javax.swing.GroupLayout.PREFERRED_SIZE))
                      .addGap(13, 13, 13)
                      .addComponent(jScrollPane1, javax.swing.GroupLayout.DEFAULT_SIZE, 147, Short.MAX_VALUE)
                      .addGap(18, 18, 18)
                      .addComponent(ReturnButton)
                      .addContainerGap())
              );

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

          private void EntAlphaActionPerformed(java.awt.event.ActionEvent evt) {
          }

          private void EntBetaActionPerformed(java.awt.event.ActionEvent evt) {
          }

          private void DecipherActionPerformed(java.awt.event.ActionEvent evt) {
              if(EntAlpha.getText().length() == 0 || EntBeta.getText().length()==0)
              {
                  TextCipher.setText("Please enter the value of alpha and beta");
                  EntAlpha.setText(null);
                  EntBeta.setText(null);
              }
              else
              {
                  int anillo=26, b, invAd = 0;
                  int alpha = Integer.parseInt(EntAlpha.getText());
                  int beta = Integer.parseInt(EntBeta.getText());
                  long[] resp = euclidesExtendido(alpha,anillo);
                  if(resp[1]<0)
                  {
                      resp[1]+=26;
                  }
                  for(b=0; b<26; b++)
                  {
                      if((b+beta)%26==0)
                      {
                          invAd=b;
                      }
                  }
                  System.out.println("Inverse multiplicative: "+resp[1]);
                  if(beta<0 || beta>26)
                  {
                      TextCipher.setText("Wrong this value cannot be accepted");
                      EntAlpha.setText(null);
                      EntBeta.setText(null);
                  }
                  else
                  {
                      char caracter, caracter1, nuevPal, c, newLet, m;
                      String mensaje = "", msjPant="";
                      int car;
                      FileReader fr = null;
                      FileWriter fw = null;
                      PrintWriter pw = null;
                      try
                      {
                          fr = new FileReader ("C:\\Users\\Daniel\\Desktop\\ESCOM\\7mo semestre\\Cryptography\\Prc4\\c.txt");
                          fw = new FileWriter("C:\\Users\\Daniel\\Desktop\\ESCOM\\7mo semestre\\Cryptography\\Prc4\\rm.txt");
                          pw = new PrintWriter(fw);
                          car = fr.read();
                          while(car != -1)
                          {

                              nuevPal= (char) (car-65);
                              m=(char) ((resp[1]*(nuevPal+invAd))%26);
                              newLet=(char) (m+97);
                              mensaje = mensaje+String.valueOf(newLet);
                              car = fr.read();
                              if(car==13 || car==10)
                              {
                                  car = fr.read();
                                  car = fr.read();
                               }
                          }
                          msjPant +=mensaje;
                          System.out.println(msjPant);
                          System.out.println("Alpha:"+alpha+" Beta: "+beta);
                          TextCipher.setText("The decrypt message is: "+ msjPant);
                          pw.println(mensaje);
                          fw.close();
                          fr.close();

                      }
                      catch(IOException e)
                      {

                      }
                  }

              }
          }
      public static long[] euclidesExtendido(long a, long b)
      {
          long[] resp = new long[3];
          long x=0,y=0,d=0;
          if(b==0)
          {
              resp[0] = a; resp[1] = 1; resp[2] = 0;
          }
          else
          {
              long x2 = 1, x1 = 0, y2 = 0, y1 = 1;
              long q = 0, r = 0;
              while(b>0)
              {
                  q = (a/b);
                  r = a - q*b;
                  x = x2-q*x1;
                  y = y2 - q*y1;
                  a = b;
                  b = r;
                  x2 = x1;
                  x1 = x;
                  y2 = y1;
                  y1 = y;
              }
              resp[0] = a;
              resp[1] = x2;
              resp[2] = y2;
          }
          return resp;
      }

```

```


        private void ReturnButtonActionPerformed(java.awt.event.ActionEvent evt) {
            new EuclideanAlgorithm().setVisible(true);
            //Cierra la ventana actual
            dispose();
        }

        public static void main(String args[]) {
            java.awt.EventQueue.invokeLater(new Runnable() {
                public void run() {
                    new Decipher().setVisible(true);
                }
            });
        }

        // Variables declaration - do not modify
        private javax.swing.JButton Decipher;
        private javax.swing.JTextField EntAlpha;
        private javax.swing.JTextField EntBeta;
        private javax.swing.JButton ReturnButton;
        private javax.swing.JTextArea TextCipher;
        private javax.swing.JLabel jLabel1;
        private javax.swing.JLabel jLabel2;
        private javax.swing.JScrollPane jScrollPane1;
        // End of variables declaration
    }
```

Euclides algorithm

```
package prc4;

public class EuclideanAlgorithm extends javax.swing.JFrame
{
    public EuclideanAlgorithm()
    {
        initComponents();
        //Centra el JFrame
        this.setLocationRelativeTo(null);
    }
    @SuppressWarnings("unchecked")
    // <editor-fold defaultstate="collapsed" desc="Generated Code">
    private void initComponents() {

        jLabel1 = new javax.swing.JLabel();
        CipherButton = new javax.swing.JButton();
        DecipherButton = new javax.swing.JButton();

        setDefaultCloseOperation(javax.swing.WindowConstants.EXIT_ON_CLOSE);
        setTitle("Euclidean Algorithm");
        setCursor(new java.awt.Cursor(java.awt.Cursor.DEFAULT_CURSOR));
        setResizable(false);

        jLabel1.setFont(new java.awt.Font("Segoe Script", 0, 18)); // NOI18N
        jLabel1.setText("Choose an option.");

        CipherButton.setFont(new java.awt.Font("Script MT Bold", 0, 12)); // NOI18N
        CipherButton.setText("Encrypt");
        CipherButton.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                CipherButtonActionPerformed(evt);
            }
        });

        DecipherButton.setFont(new java.awt.Font("Script MT Bold", 0, 12)); // NOI18N
        DecipherButton.setText("Decrypt");
        DecipherButton.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                DecipherButtonActionPerformed(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()
                .addGap(80, 80, 80)
                .addComponent(jLabel1)
                .addContainerGap(90, Short.MAX_VALUE))
            .addGroup(layout.createSequentialGroup()
                .addGap(62, 62, 62)
                .addComponent(CipherButton)
                .addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED, javax.swing.GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE)
                .addComponent(DecipherButton)
                .addGap(54, 54, 54))
        );
        layout.setVerticalGroup(
            layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addGroup(layout.createSequentialGroup()
                .addGap(20, 20, 20)
                .addComponent(jLabel1)
                .addGap(53, 53, 53)
                .addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.BASELINE)
                    .addComponent(CipherButton)
                    .addComponent(DecipherButton))
                .addContainerGap(84, Short.MAX_VALUE))
        );

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

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

        //Abre JFrame Cipher
        new Decipher().setVisible(true);
       //Cierra la ventana actual
       dispose();
    }

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

       //Abre JFrame Cipher
        new Cipher().setVisible(true);
       //Cierra la ventana actual
       dispose();
    }

    /**
     * @param args the command line arguments
     */
    public static void main(String args[]) {
        java.awt.EventQueue.invokeLater(new Runnable()
        {
            public void run()
```

```java
            {
                new EuclideanAlgorithm().setVisible(true);
            }
        });
    }

           // Variables declaration - do not modify
           private javax.swing.JButton CipherButton;
           private javax.swing.JButton DecipherButton;
           private javax.swing.JLabel jLabel1;
           // End of variables declaration
       }
```