UF1. [PAC01] CRIPTOGRAFÍA

Actividades

Parte teórica

1. Cifra el mensaje "HOLA, QUE TAL" con un desplazamiento de 6 caracteres y contesta, justificando tus respuestas, a las siguientes preguntas:

Para cifrar el mensaje aplicando un desplazamiento de 6 caracteres, a cada letra del abecedario le asignamos la letra desplazada de 6 posiciones, es decir, la A se correspondería con la G; la B con la H, y así sucesivamente, lo que podríamos escribir como:

$$C(x) = x + 6 \bmod 27$$

Dónde x sería cualquiera de las 27 letras del abecedario castellano, C(x), su correspondencia una vez cifrada (aplicado el desplazamiento de 6) y módulo 27, porque el alfabeto sólo tiene 27 letras, por lo que una vez lleguemos a la U+6, volveríamos a la A. Por ejemplo la W sería la B, y así sucesivamente.

   a. ¿Cuál es el texto cifrado resultante?

NUQG, WAK ZGQ

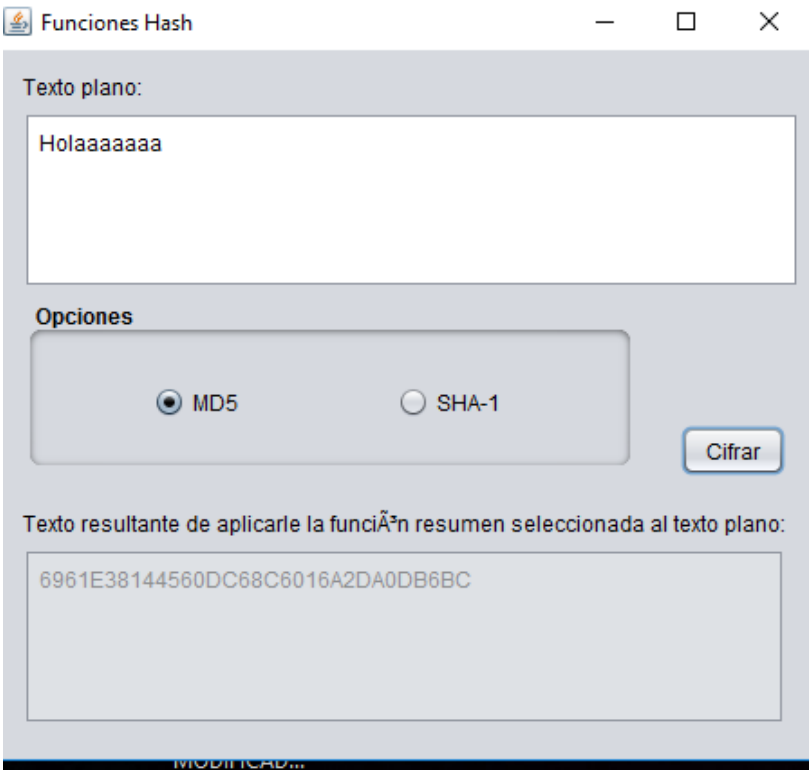
   b. ¿Y si lo desplazamos 27?

Como el alfabeto castellano tiene 27 letras, realizar un desplazamiento de 27 letras nos daría el mismo mensaje original, es decir, el mensaje cifrado sería idéntico al original.

Parte práctica

2. Escribe un programa en el que podamos introducir un texto y mediante una selección se pueda escoger cifrar este texto en MD5 o SHA-1 y muestre el resultado en HEXADECIMAL.

   Propuesta de diseño:




```
package FuncionesResumen.src.my.funcionesresumen;

import java.security.*;

/**
 *
 * @author Ana
 */
public class FuncionesHash extends javax.swing.JFrame {

    /**
     * Creates new form FuncionesResumenUI
     */
    public FuncionesHash() {
        initComponents();
        jRadioButton1.setSelected(rootPaneCheckingEnabled);
    }

    /**
     * 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() {
```

```
        buttonGroup1 = new javax.swing.ButtonGroup();
        jLabel1 = new javax.swing.JLabel();
        jScrollPane1 = new javax.swing.JScrollPane();
        jTextArea1 = new javax.swing.JTextArea();
        jPanel1 = new javax.swing.JPanel();
        jRadioButton1 = new javax.swing.JRadioButton();
        jRadioButton2 = new javax.swing.JRadioButton();
        jButton1 = new javax.swing.JButton();
        jScrollPane2 = new javax.swing.JScrollPane();
        jTextArea2 = new javax.swing.JTextArea();
        jLabel2 = new javax.swing.JLabel();

        setDefaultCloseOperation(javax.swing.WindowConstants.EXIT_ON_CLOSE);
        setTitle("Funciones Hash");

        jLabel1.setText("Texto plano:");

        jTextArea1.setColumns(20);
        jTextArea1.setRows(5);
        jScrollPane1.setViewportView(jTextArea1);


jPanel1.setBorder(javax.swing.BorderFactory.createTitledBorder("Opciones"));

        buttonGroup1.add(jRadioButton1);
        jRadioButton1.setText("MD5");

        buttonGroup1.add(jRadioButton2);
        jRadioButton2.setText("SHA-1");
        jRadioButton2.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                jRadioButton2ActionPerformed(evt);
            }
        });

        javax.swing.GroupLayout jPanel1Layout = new
javax.swing.GroupLayout(jPanel1);
        jPanel1.setLayout(jPanel1Layout);
        jPanel1Layout.setHorizontalGroup(

jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addGroup(jPanel1Layout.createSequentialGroup()
                .addGap(58, 58, 58)
                .addComponent(jRadioButton1)

.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED, 88,
Short.MAX_VALUE)
                .addComponent(jRadioButton2)
                .addGap(62, 62, 62))
        );
        jPanel1Layout.setVerticalGroup(

jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addGroup(jPanel1Layout.createSequentialGroup()
                .addGap(19, 19, 19)
```

```
.addGroup(jPanel1Layout.createParallelGroup(javax.swing.GroupLayout.Alignment
.BASELINE)
                    .addComponent(jRadioButton1)
                    .addComponent(jRadioButton2))
                .addContainerGap(18, Short.MAX_VALUE))
        );

        jButton1.setText("Cifrar");
        jButton1.addActionListener(new java.awt.event.ActionListener() {
            public void actionPerformed(java.awt.event.ActionEvent evt) {
                jButton1ActionPerformed(evt);
            }
        });

        jTextArea2.setColumns(20);
        jTextArea2.setRows(5);
        jTextArea2.setEnabled(false);
        jScrollPane2.setViewportView(jTextArea2);

        jLabel2.setText("Texto resultante de aplicarle la funciÃ³n resumen
seleccionada al texto plano:");

        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(19, 19, 19)

.addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADIN
G)
                    .addComponent(jScrollPane1,
javax.swing.GroupLayout.Alignment.TRAILING)
                    .addGroup(layout.createSequentialGroup()

.addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADIN
G)
                            .addComponent(jLabel2)

.addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.TRAILI
NG, false)
                                .addGroup(layout.createSequentialGroup()
                                    .addComponent(jPanel1,
javax.swing.GroupLayout.PREFERRED_SIZE, javax.swing.GroupLayout.DEFAULT_SIZE,
javax.swing.GroupLayout.PREFERRED_SIZE)

.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED, 24,
Short.MAX_VALUE)
                                    .addComponent(jButton1))
                                .addComponent(jScrollPane2,
javax.swing.GroupLayout.Alignment.LEADING)
                                .addComponent(jLabel1,
javax.swing.GroupLayout.Alignment.LEADING)))
```

```
                        .addGap(0, 8, Short.MAX_VALUE)))
                .addContainerGap())
        );
        layout.setVerticalGroup(

layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addGroup(layout.createSequentialGroup()
                .addGap(12, 12, 12)
                .addComponent(jLabel1)

.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED)
                .addComponent(jScrollPane1,
javax.swing.GroupLayout.PREFERRED_SIZE, javax.swing.GroupLayout.DEFAULT_SIZE,
javax.swing.GroupLayout.PREFERRED_SIZE)
                .addGap(7, 7, 7)

.addGroup(layout.createParallelGroup(javax.swing.GroupLayout.Alignment.TRAILI
NG)
                    .addComponent(jPanel1,
javax.swing.GroupLayout.PREFERRED_SIZE, javax.swing.GroupLayout.DEFAULT_SIZE,
javax.swing.GroupLayout.PREFERRED_SIZE)
                    .addComponent(jButton1))
                .addGap(18, 18, 18)
                .addComponent(jLabel2)

.addPreferredGap(javax.swing.LayoutStyle.ComponentPlacement.RELATED)
                .addComponent(jScrollPane2,
javax.swing.GroupLayout.PREFERRED_SIZE, javax.swing.GroupLayout.DEFAULT_SIZE,
javax.swing.GroupLayout.PREFERRED_SIZE)
                .addContainerGap(19, Short.MAX_VALUE))
        );

        pack();
    }// </editor-fold>//GEN-END:initComponents

    private void jButton1ActionPerformed(java.awt.event.ActionEvent evt)
{//GEN-FIRST:event_jButton1ActionPerformed
        // TODO add your handling code here:

        MessageDigest md;
        String algorithm;

        //Siempre estarÃ¡ seleccionado uno u otro, ya que lo hemos
inicializado
        if (jRadioButton1.isSelected())
            algorithm="MD5";
        else
            algorithm="SHA1";

        try {
           md = MessageDigest.getInstance(algorithm);

           //Capturamos el texto
           String texto = jTextArea1.getText();

           //Convertimos el texto a bytes
```

```
            byte dataBytes[] = texto.getBytes();
            //Se introduce el texto en bytes a resumir
            md.update(dataBytes);
            //Se calcula el resumen
            byte resumen[] = md.digest();

            String salida = Hexadecimal(resumen);

            jTextArea2.setText(salida);

        }catch (NoSuchAlgorithmException e){
            e.printStackTrace();
        }

    }//GEN-LAST:event_jButton1ActionPerformed

    static String Hexadecimal(byte[] resumen){
        String hex = "";
        for (int i = 0; i<resumen.length; i++){
            String h = Integer.toHexString(resumen[i] & 0xFF);
            if (h.length()==1) hex +=0;
            hex += h;
        }

        return hex.toUpperCase();
    }

    private void jRadioButton2ActionPerformed(java.awt.event.ActionEvent evt)
{//GEN-FIRST:event_jRadioButton2ActionPerformed
        // TODO add your handling code here:
    }//GEN-LAST:event_jRadioButton2ActionPerformed

    /**
     * @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(FuncionesHash.class.getName()).log(java.ut
il.logging.Level.SEVERE, null, ex);
        } catch (InstantiationException ex) {

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

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

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

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

    // Variables declaration - do not modify//GEN-BEGIN:variables
    private javax.swing.ButtonGroup buttonGroup1;
    private javax.swing.JButton jButton1;
    private javax.swing.JLabel jLabel1;
    private javax.swing.JLabel jLabel2;
    private javax.swing.JPanel jPanel1;
    private javax.swing.JRadioButton jRadioButton1;
    private javax.swing.JRadioButton jRadioButton2;
    private javax.swing.JScrollPane jScrollPane1;
    private javax.swing.JScrollPane jScrollPane2;
    private javax.swing.JTextArea jTextArea1;
    private javax.swing.JTextArea jTextArea2;
    // End of variables declaration//GEN-END:variables
}
```