v.8.4

Trabajo Práctico Final - Tema 3

Programación I

1 Criptografía

La Criptografía se encarga del estudio de técnicas para intercambiar información de forma segura frente a la presencia de terceras partes (llamadas normalmente adversarios). Es un área importante y con muchas aplicaciones dentro de las ciencias de la computación, en particular en lo referido a seguridad informática.

1.1 El cifrado del César

El Cifrado del César es un mecanismo de criptografía simétrica muy simple, en la cual el emisor y el receptor utilizan una clave previamente conocida para codificar y decodificar mensajes.

Una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etc. Este método debe su nombre a Julio César, que lo usaba para comunicarse con sus generales. El valor de desplazamiento es la clave del método.

Ejercicio 1. En el archivo cesar-subir.rkt se encuentra una implementación incompleta del método del César. Se pide completar las definiciones faltantes. Puede además incorporar todas las funciones auxiliares que crea conveniente.

Al terminar, si definimos estas constantes

```
(define ALFABETO "ABCDEFGHIJKLMNÑOPQRSTUVWXYZ 0123456789")
(define CLAVE 3)
(define CODIGO-DEL-CESAR (cifrado CLAVE ALFABETO))
```

y evaluamos las siguientes expresiones

```
(encriptar-mensaje "HOLA" ALFABETO CLAVE)
(encriptar-mensaje "ATACAR A LAS 18" ALFABETO CLAVE)
(encriptar-mensaje "LA OPERACION ES REVERSIBLE" ALFABETO CLAVE)
(desencriptar-mensaje (encriptar-mensaje "LA OPERACION ES REVERSIBLE" ALFABETO CLAVE) ALFABETO CLAVE)
```

obtenemos

```
"KRÑD"
"DWDFDU2D2ÑDV24B"
"ÑD2RSHUDFLRP2HV2UHYHUVLEÑH"
"LA OPERACION ES REVERSIBLE"
```

2 Formato de entrega

- El trabajo práctico debe resolverse en grupos de hasta dos integrantes. Cada persona puede participar en un único grupo.
- Exactamente una persona por grupo debe realizar la entrega en el sitio, escribiendo en el campo "Comentarios" los apellidos y nombres de cada integrante.
- No se aceptarán entregas en las que no se haya seguido la receta para el diseño. Para que la entrega del trabajo práctico sea válida, todas las funciones deben contar con diseño de datos, signatura, declaración de propósito, casos de prueba (si corresponde) y código. En caso contrario, se considerará que el TP no fue entregado.
- La entrega consiste en un único archivo por grupo: el archivo TP5-Apellido1-Apellido2.rkt que deberá ser editado apropiadamente. En concreto, se solicita:
    - Completar los datos pedidos para cada integrante del grupo según se indica en el archivo.
    - Completar el archivo con la resolución.
    - Cambiar el nombre del archivo reemplazando Apellido1 y Apellido2 por los apellidos de los integrantes.