Monestir de Poblet, s/n 46015 - Valencia
46022257@edu.gva.es Tl. 96 1206100

Ej1 a (3 puntos)

Crear la clase UiCypher que debe tener dos propiedades mascField y shiftField que son cada uno de ellos un randomField. mascFild debe generar números entre 1 y 1000000. shiftField debe generar números entre 1 y 25.

El constructor de esta clase no requiere ningún parámetro.

Crear la clase Cypher sin parámetros que debe tener en su interfaz pública una tabla, con dos textareas, dos botones y un array de cyphers (se explica en el punto c)

La clase Cypher debe tener un método público addRow que al llamarlo debe añadir una nueva fila en la tabla con un nuevo UiCypher. (o sea, dos campos randomField con sus botones generadores)

Ej 1 b (1 punto)

En el constructor se debe de crear una fila inicial con un UiCypher en la fila y en la última celda un botón de añadir. Al hacer clic a añadir se debe utilizar el método addRow para añadir una nueva fila a la tabla.

Ej1 c (2 puntos)

Añadir el evento al botón encriptar.

Para ello cuando se haga clic a encriptar:

Se debe coger el texto del primer textarea y convertirlo en mayúsculas.

Se debe de crear un CesarCypher por cada UiCypher de la tabla (la clase CesarCypher se facilita).

Con el texto en mayúsculas se debe de llamar al método crypt del primer CesarCypher y su salida, que es nuevamente un texto, se le debe de pasar al siguiente método crypt del siguiente CesarCypher y así sucesivamente hasta el último.

El texto resultante se debe poner en el segundo textarea.

Ej1 d (1 punto)

Añadir el evento al botón desencriptar.

Para ello cuando se haga clic a desencriptar:

Se debe coger el texto del segundo textarea y convertirlo en mayúsculas.

Se debe de crear un CesarCypher por cada UiCypher de la tabla (la clase CesarCypher se facilita).

Monestir de Poblet, s/n 46015 - Valencia
46022257@edu.gva.es Tl. 96 1206100

Con el texto en mayúsculas se debe de llamar al método decrypt del primer CesarCypher y su salida, que es nuevamente un texto, se le debe de pasar al siguiente método decrypt del siguiente CesarCypher y así sucesivamente hasta el último.

El texto resultante se debe poner en el primer textarea.

NOTA: Si no se ha hecho el ej1b. Se puede realizar el ej1 c y d considerando que solo hay un UiCypher y por tanto directamente crear un único CesarCypher encriptar/descriptar y mostrar el resultado en el correspondiente textarea. En este caso, la nota máxima del ej1 c y d será 2 puntos.

Ej 2 (3 puntos)

Generar la clase CesarCypher

Parámetros:

mascara: número que se convertirá en binario y se utilizará para calcular el desplazamiento en el cifrado/descifrado. Se debe almacenar en el parámetro público masc.

Desplazamiento: número que se utiliza para calcular el desplazamiento en el cifrado/descifrado. Se debe almacenar en el parámetro público shift.

Métodos públicos:

crypt: requiere un parámetro que es un texto en mayúsculas y con espacios. Devuelve la cadena cifrada según la función de cifrado. Se debe utilizar tranform para obtenerla.

decrypt: requiere un parámetro que es un texto en mayúsculas y con espacios. Devuelve la cadena descifrada según la función de descifrado. Se debe utilizar tranform para obtenerla.

Métodos privados: hay facilitados dentro del código inicial.

function toBinary(num), var charCodeAt = function(letter), var _crypt = function(number) y var numberToChar=function(number).

Y a realizar por el alumno:

letterCrypt: Función que realiza el cifrado/descifrado de un carácter (ver explicación al final)

*@param {[string]} letter: cadena de una sola letra

Monestir de Poblet, s/n 46015 - Valencia
46022257@edu.gva.es Tl. 96 1206100

@param {[number]} pos: posición dentro del texto donde se encuentra la letra letter

@param {[boolean]} type: si type es true indica que debe cifrar la letra letter. Si type es false indica que debe descifrar la letra letter

*@return {[string]} cadena de una sola letra cifrada/descifrada a partir de los valores masc y shift con un cesar enmascarado

transform: función que devuelve las funciones de cifrado/descifrado. Pasando type a true debe devolver la función de cifrado de un texto y con false debe devolver la función de descifrado del texto

* @param {[boolean]} type parámetro boolean que se le pasa a f

* @param {[function]} f función de tipo letterCrypt(letter,pos,type)

* @return {[function]} función que requiere un texto y devuelve el texto cifrado/descifrado utilizando la función f. Para ello debe recorrer el texto y llama a la función f por cada carácter

Algoritmo Cesar enmascarado con desplazamiento:

El algoritmo Cesar consiste en dada una letra p.e. A y un número p.e. 3, se devuelve la letra que en abecedario está 3 posiciones después. En este caso la D. La cadena "AB A" devolvería "DE D". Los espacios no deben de modificarse.

EL algoritmo enmascarado trabaja con una máscara que es un número que convertimos a binario. P.e mascara=6 que binario es 110. Para el caso anterior desplazamiento 3. Ahora se calculan los desplazamientos teniendo en cuenta la posición en el texto de la letra y la máscara. Así para el texto "ABBA" daría lo siguiente

Posicon 0: A . Se mira la posicon0 del binario de 6, que es 1 y se le suma al desplazamiento 3. Por tanto, se suma 4 y la letra encriptada es E.

Posicon 1: B . Se mira la posicon1 del binario de 6, que es 1 y se le suma al desplazamiento 3. Por tanto, se suma 4 y la letra encriptada es F.

Posicon 2: B . Se mira la posicon2 del binario de 6, que es 0 y se le suma al desplazamiento 3. Por tanto, se suma 3 y la letra encriptada es E.

Posicon 3: A . Se mira la posicon3 del binario de 6. Como 3la longitud del binario se vuelve a la poscion 0(o sea se hace el módulo de la longitud de 110) que es 1 y se le suma al desplazamiento 3 . Por tanto, se suma 4 y la letra encriptada es E.

La cadena encriptada de ABBA es EFEE

Monestir de Poblet, s/n 46015 - Valencia
46022257@edu.gva.es Tl. 96 1206100

El proceso de desencriptación es igual, pero en vez de sumar, se resta el desplazamiento. Veamos en el último caso, la última letra:

Posición 3: E . Se mira la posicon3 del binario de 6. Como 3 es la longitud del binario se vuelve a la posición 0(o sea se hace el módulo de la longitud de 110) que es 1 y se le suma al desplazamiento 3 . Por tanto, **se resta 4** y la letra encriptada es A.

Esta forma con tan poca diferencia de encriptar/desencriptar permite hacerlo con una sola función que según un booleano haga suma o haga resta.

Consideraciones de la calificación del examen:

1. El uso de variables globales o identificadores innecesarios será penalizado como ejercicio incorrecto.
2. Siempre será considerada mejor solución aquella que esté realizada siguiendo las pautas marcadas en el enunciado. Por tanto, aquellas soluciones que difieran de la mejor penalizaran en su corrección.
3. Si se presenta una solución que funciona, pero no está realizada según se ha planteado en el enunciado, se considerará como incorrecta y penalizará según las diferencias con respecto a las pautas indicadas en los enunciados.
4. El sistema de calificación es por resta de puntuación según valor de penalización de los errores cometidos.
5. La realización del examen es individual y sin conexión a internet/red. Cualquier copia será califica con 0 y el alumno perderá el derecho a evaluación continua.
6. El alumno dispondrá de los materiales del curso y sus prácticas personales, así como de manuales de referencia offline que disponga en su ordenador de aula. Cualquier consulta de otro material, por parte del alumno, será considerada como copia.
7. El alumno entregará un fichero zip nombrado con su nombre y primer apellido donde debe incluir los ficheros modificados del examen en el usb que debe tener conectados durante todo el examen. El alumno firmará la hoja de asistencia al examen que acredita que hace la entrega de este fichero zip en el ordenador del profesor.

Monestir de Poblet, s/n 46015 - Valencia
46022257@edu.gva.es Tl. 96 1206100