Criptografía

En el presente ejercicio se pide desarrollar una aplicación que permita cifrar mensajes haciendo uso de diferentes tipos de cifrado.

Por una parte, los de **sustitución**. Es un método de cifrado por el cual, unidades de texto plano son sustituidas con texto cifrado siguiendo un sistema regular. Las "unidades" pueden ser una sola letra, pares de letras o tríos de letras, entre otros. Por ejemplo:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	...
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	
x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	...

Donde la palabra “hola”, se cifraría como “elix”.

Por otra parte, se hará uso del tipo de cifrado por transposición, en el cual unidades de texto plano se cambian de posición siguiendo un esquema bien definido. Existen diferentes variantes dentro los cifrados por transposición. En el presente ejercicio se hará uso de la **transposición por grupos** y de la **transposición por series**.

En cuanto a la transposición por grupos, los caracteres del texto se reordenan por medio de una permutación de un conjunto de caracteres que se repite constantemente. Ejemplo: utilizando la permutación 24531, la palabra “COMPLICADO” se cifraría como “OPLMCCDOAI” (OPLMC CDOAI).

Por último, en la transposición por series se hará uso de tres series diferentes para el cifrado del mensaje. Primero un listado de los primeros N números primos. A continuación, los N primeros números pares no primos. Finalmente, los N primeros números impares no primos. Donde N sería la longitud del mensaje que se desea cifrar. Ejemplo para un mensaje de 20 caracteres de longitud:

Primos:	1	2	3	5	7	11	13	17	19
Pares:	4	6	8	10	12	14	16	18	20
Impares:	9	15							

Junto al enunciado, se proporciona un pequeño esqueleto de la aplicación. Para definir el algoritmo de sustitución y el de transposición por grupos, se hará uso de la Clase Random. Para trabajar con el algoritmo de transposición por series, se hará uso de Listas.

A continuación, se muestra una captura de pantalla con la apariencia deseada. Tres *RadioButton* para cada uno de los tipos de cifrado. El campo longitud del grupo, únicamente será visible cuando se seleccione la opción de "transposición por grupos". Un *TextBox* que permita introducir un texto. Y otros dos TextBox para mostrar el texto cifrado. Así, se deberá de codificar el correspondiente método para descifrar el mensaje, y de esta forma, comprobar si el cifrado se ha realizado correctamente.

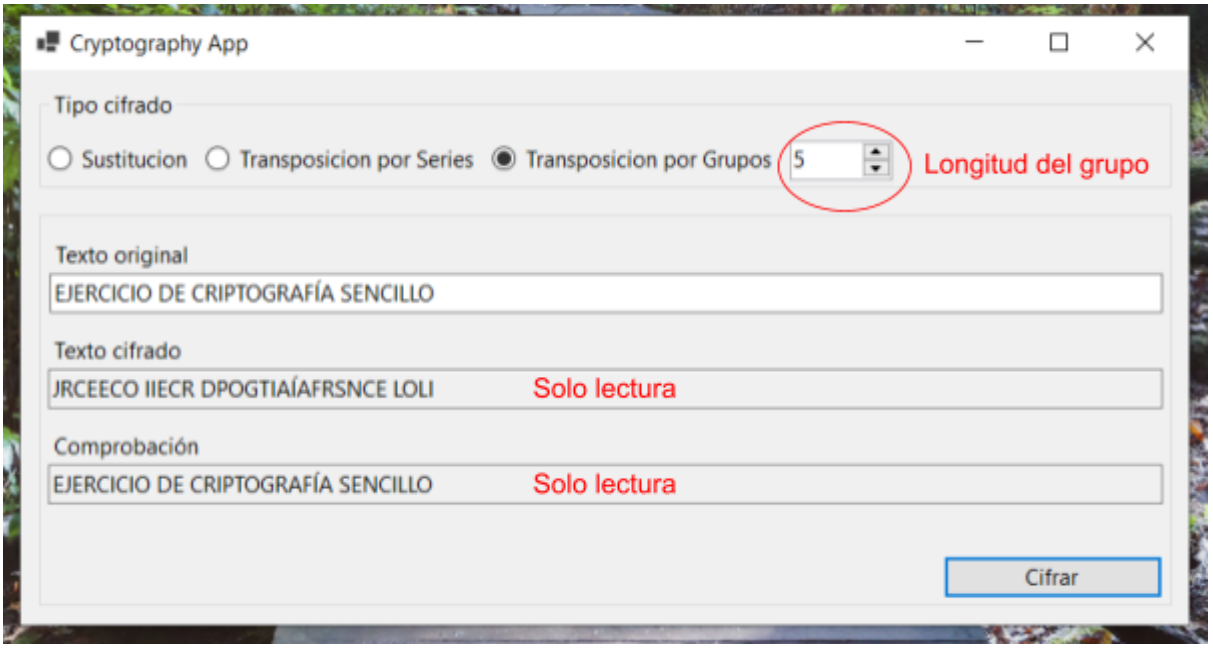

figura 1.1

NOTA 1: Los mensajes se introducirán únicamente en mayúsculas. En el algoritmo de sustitución se realizará haciendo uso de unidades de un único carácter (A-Z). Si algún carácter de sustitución no existe, no se reemplazará.

RECORDAD: Códigos ASCII.