PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
ESTUDIOS GENERALES CIENCIAS

TÉCNICAS DE PROGRAMACIÓN

Laboratorio N° 5

Semestre académico 2014-1

Advertencia N°1: Está prohibido el acceso a Internet y a correo electrónico hasta que lo indiquen los jefes de práctica. Grabe el archivo en la dirección que los jefes de práctica indiquen, en la Intranet del curso. Use el formato de nombre de archivo que se le indique, caso contrario **NO SE CORREGIRÁ** su trabajo y se le asignará la nota cero (00).

Advertencia N°2: LAS SOLUCIONES DEBERÁN DESARROLLARSE BAJO UN ESTRICTO DISEÑO DESCENDENTE, por lo que NO SE CALIFICARÁN aquellos módulos que son llamados por otros que estén incompletos. Cada módulo no debe sobrepasar las 20 líneas aproximadamente.

En ninguna de las preguntas se podrá utilizar funciones, procedimientos u operadores que manejen cadenas de caracteres y si emplean variables de tipo String, estas no podrán ser manipuladas como arreglos. No se podrán emplear archivos intermedios ni variables globales. Finalmente no se podrán emplear bibliotecas de funciones que no sean las incorporadas en el núcleo de Pascal, por lo que no se puede emplear la clausula "uses" en los programas. De incumplir esto se anulará la pregunta.

Hoy en día la información que se transmite a través de medios electrónicos es muy susceptible de ser capturada por terceros y que le den mal uso. Por esa razón que existen muchos métodos que permiten cifrar la información que se envíe de modo que si alguien la captura no lo pueda entender.

En este laboratorio se quiere que usted elabore un conjunto de programas que permitan de manera automatizada cifrar y descifrar mensajes de texto. El método que se empleará es una variante del método que utilizó Julio César en la antigua Roma y que recibe precisamente el nombre de "Método César" o "Método de desplazamiento". El método se describe a continuación:

- En un archivo de textos se guarda en la primera línea la lista de caracteres que se van a emplear en los mensajes a cifrar (no necesariamente están todos los caracteres de la tabla ASCII), en la segunda línea se colocan una serie de valores enteros, la cantidad de valores puede variar entre 3 y 12, y los valores pueden ir desde 2 a n-2, siendo n el número de caracteres que se colocó en la primera línea. El archivo es similar al siguiente:

```
ABCDEFG...WXYZabcd...xyz0123..89_,;:-+...()&?
5  12 7  23 19  3  35 ...
```

  A este archivo se le conoce como "el archivo que contiene la clave para cifrar o descifrar los mensajes" y sólo lo debe tener la persona que envía el mensaje y aquella a la que se le envía el mensaje y que por medio de ella podrá descifrarlo.

- El algoritmo luego empieza a leer uno a uno los caracteres de otro archivo que contiene el mensaje y a cada carácter se le aplica una transformación como se explica a continuación:
  - Se toma el primer número del archivo (en el ejemplo 5) y luego se procede a "girar" o "desplazar" el alfabeto tantos caracteres como indica el número, esto es:

Alfabeto original →	A	B	C	D	E	F	G	H	I	...	K	(	)	&	?
Alfabeto "girado" →	E	F	G	H	I	J	K	L	M	...	?	A	B	C	D

  - Se ubica el carácter en el alfabeto original y se toma el caracter que se encuentra en la misma posición en el alfabeto girado. Ese caracter se coloca en otro archivo que guardará el mensaje cifrado, por ejemplo si el carácter leído fuera 'G', el carácter escrito sería 'K'.

Alfabeto original →	A	B	C	D	E	F	**G**	H	I	...	K	(	)	&	?
							↓								
Alfabeto "girado" →	E	F	G	H	I	J	**K**	L	M	...	?	A	B	C	D

  - Luego se procede de manera similar con el siguiente caracter del mensaje y el siguiente número. Si los números se acabasen, se les vuelven a tomar desde el principio.
  - Si un carácter del mensaje no se encontrara en el alfabeto se guarda en el mensaje sin modificar.

Continúa...

Se pide:

Pregunta 1 (7 puntos)

Escriba un programa que permita generar el archivo von la clave. Para esto deberá seguir el siguiente proceso:

- Se toma un archivo de textos relativamente grande y de él se extraen todos los caracteres sin repetir que haya en él. Estos caracteres conformarán el alfabeto original. Luego para que el descifrado del mensaje sea un poco más complicado de descifrar, se procede a desordenar estos caracteres.
- Se genera un número aleatorio (r) entre 3 y 12
- Luego se generan "r" números aleatorios entre 2 a n-2, siendo "n" el número de caracteres del alfabeto original. Estos números debe ser diferentes entre sí.
- Se guarda el alfabeto y la lista de números en el archivo clave.

Los archivos que se empleen en este programa pueden cambiar a cada momento, por lo que no podrá emplear nombres fijos para denominarlos. El archivo con el texto no podrá cargarse en su totalidad en la memoria del computador y sólo se podrá leer una vez.

Pregunta 2 (6.5 puntos)

Elabore un programa que permita cifrar un mensaje que se encuentre en un archivo de textos empleando el método descrito anteriormente con la clave generada en el programa de la pregunta 1. Los nombres de los archivos no pueden ser fijos. El archivo con el mensaje sólo se podrá leer una vez.

Pregunta 3(6.5 puntos)

Elabore un programa que permita descifrar un mensaje cifrado que se encuentre en un archivo de textos empleando el método descrito anteriormente con la clave generada en el programa de la pregunta 1. Esto quiere decir que si el programa se aplica al archivo generado en la pregunta 2 se debe obtener un archivo idéntico al del mensaje inicial. Los nombres de los archivos no pueden ser fijos. El archivo con el mensaje sólo se podrá leer una vez.

Lima, 11 de mayo del 2014.