Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación
Lenguajes de Programación (6204)
Semestre 2-2019

Proyecto #1 – Haskell

Existen diferentes maneras de cifrar un mensaje; los más conocidos, también conocidos como cifrados clásicos incluyen: el cifrado César, el cifrado Atbash y cifrado de Vigenère. En este proyecto Ud. debe crear, para cada tipo de cifrado mencionado, una función que codifique y otra que descodifique.

En el **cifrado César** cada letra en el texto original es reemplazada por otra letra que se encuentra n posiciones más adelante en el alfabeto. Por ejemplo, la codificación con un desplazamiento 3 del mensaje “en todo la medida” es “hq wrgr od phglgd” y la codificación con un desplazamiento 5 de “en todo la medida” es “js ytit qf rjinif”. La descodificación de un texto codificado con un desplazamiento n se obtiene codificándolo con un desplazamiento –n.

```
cesarCod :: Int -> String -> String
cesarDes :: Int -> String -> String
```

En el **cifrado Atbash** Se le denomina también método de espejo, pues consiste en sustituir la primera letra por la última, la segunda por la penúltima y así sucesivamente.

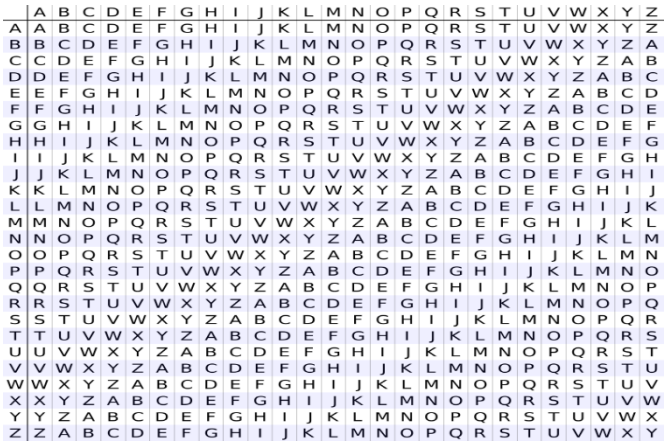
Original	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrado	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

```
atbash :: String -> String
```

Nota: en el cifrado Atbash no se necesita una función que descodifique, ya para descodificar se puede usar la misma función.

El **cifrado Vigenère** es un cifrado basado en diferentes series de caracteres o letras del cifrado César, formando estos caracteres una tabla (tabla de Vigenère). Este tipo de cifrado usa una palabra clave para codificar el texto. Para realizar este cifrado primero cada letra del texto original se le corresponde una letra de la palabra clave, siguiendo el orden de la clave y se repite la clave hasta que cada letra del texto le corresponda una letra de la clave. Luego para cada letra del texto se usa la tabla para cifrar esa letra, siendo: la letra del texto, la coordenada de la columna y la letra de la clave, la coordenada de la fila. Finalmente, la letra que corresponde a esas coordenadas es la letra de cifrada. Para descodificar se sigue el proceso inverso.

Tabla:



Ejemplo:

Siendo la Frase Original “attack at dawn” y la clave “Lemon”, se codifica de la siguiente forma:
Se escribe cada palabra de la frase original usando solo las letras de la palabra clave en orden dando “lemonl em onle”, luego se usan las primeras letras de estas dos frases, “a” y “l” en la tabla y nos da “l” y si seguimos para todas las letras nos da la frase “lxfopv ef rnhr”.

Original:	`attack at dawn`
Palabra clave (“Lemon”):	`LemonL em onLe`
Cifrado:	`lxfopv ef rnhr`

Para descodificarlo se hace el proceso inverso se usan las frases “lemonl em onle” y “lxfopv ef rnhr”, luego se usan las primeras letras de estas dos frases, “l” y “l”, buscamos en la fila “l” (la cual es la primera letra de la clave) la letra “l” (la primera letra de la frase cifrada) y escribimos la primera letra de esa columna “a”, en la segunda letra se busca la letra “x” en la fila “e” la cual está en la columna “t” y así dando “attack at dawn”.

```
vigenereCod:: String -> String -> String
vigenereDes:: String -> String -> String
```

(Donde el primer String es la frase a codificar/descodificar y el segundo String es la clave)

Consideraciones

- En los algoritmos de cifrado solo se codifican/descodifican los caracteres en los rangos ‘a’-’z’ y ‘A’-’Z’. Cualquier caracter que no pertenezca a estos rangos permanece sin cambios en el texto de salida.
- El desplazamiento en algoritmos como el César, son circulares.
- Sólo puede utilizar operaciones del Prelude de Haskell y se espera el uso preferente de funciones de orden superior.
- La entrega del proyecto será el lunes 16/12/2019

- El resto de las consideraciones se encuentran en el documento “Condiciones de Entrega”.

GDLP, Nobiembre 2019