ALGORITMOS Y PROGRAMACIÓN
PROYECTO 1 – LA CIFRA VIGENÈRE

Desde años remotos se ha querido disfrazar la forma de comunicarse enviando mensajes con significados ocultos. Desde declaraciones de amor, hasta los planes de batalla se enviaban usando técnicas que hicieran posible el intercambio de mensajes de manera segura para que sólo pudieran ser leídos por las personas a quienes iban dirigidos.

La encriptación o codificación de mensajes, es el procedimiento con más confianza para intercambiar información de manera segura. Por lo general, la aplicación concreta de la encriptación se basa en la existencia de una *clave*. Básicamente consiste en "disfrazar" o codificar un mensaje de forma tal que sólo lo pueda descifrar quien posea la clave de desencriptación.

Existen numerosos métodos de encriptación que han sido inventados desde los principios de la escritura, uno de estos métodos es “La cifra de Vigenère”.

La cifra de Vigenère es un método basado en el ¨cifrado de Alberti¨ que consistía en utilizar dos o más alfabetos **alternando entre ellos durante la codificación**, confundiendo de esta manera a los potenciales criptoanalistas.

Alfabeto llano	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
Alfab. cifrado 1	F Z B V K I X A Y M E P L S D H J O R G N Q C U T W
Alfab. cifrado 2	G O X B F W T H Q I L A P Z J D E S V Y C R K U H N

Por ejemplo, aquí tenemos dos posibles alfabetos cifrados, y podríamos cifrar un mensaje alternando entre ellos. Para cifrar el mensaje ***"aquello"***, codificaríamos la primera letra según el primer alfabeto cifrado, de forma que **a** se convierte en **F**, pero codificaríamos la segunda letra según el segundo alfabeto cifrado, de forma que q se convierte en E. Para cifrar la tercera letra volvemos al primer alfabeto cifrado, para la cuarta acudimos al segundo alfabeto cifrado, y así sucesivamente. Esto significa que u es codificada como N, e como F, la primera l como P, mientras que la segunda l se convierte en A, y la o final en D. El texto cifrado completo sería FENFPAD.

La fuerza de la cifra Vigenère radica en que no utiliza uno, sino que tiene un alfabeto llano seguido de 26 alfabetos cifrados distintos, para cifrar un mensaje. El primer paso de la codificación es tener lo que se denomina conjunto de alfabetos de codificación Vigenère, este conjunto de alfabetos son:

Alfabeto	llano	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
Alfab. cifrado	1	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	A
Alfab. cifrado	2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
Alfab. cifrado	3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
Alfab. cifrado	4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
Alfab. cifrado	5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
Alfab. cifrado	6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
Alfab. cifrado	7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
Alfab. cifrado	8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
Alfab. cifrado	9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
Alfab. cifrado	10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
Alfab. cifrado	11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
Alfab. cifrado	12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
Alfab. cifrado	13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Alfab. cifrado	14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Alfab. cifrado	15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Alfab. cifrado	16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Alfab. cifrado	17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Alfab. cifrado	18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Alfab. cifrado	19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Alfab. cifrado	20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
Alfab. cifrado	21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
Alfab. cifrado	22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Alfab. cifrado	23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Alfab. cifrado	24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Alfab. cifrado	25	Z	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
Alfab. cifrado	26	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

Para cifrar el mensaje debe establecerse una clave entre el emisor y el receptor del mensaje. Por ejemplo, tómese la palabra “HIELO” como clave para codificar el mensaje “DESVIE TROPAS A LA LOMA OESTE”, texto cifrado quedaría de la siguiente manera.

Clave	H	I	E	L	O	H	I	E	L	O	H	I	E	L	O	H	I	E	L	O	H	I	E				
Texto llano	d	e	s	v	i	e	t	r	o	p	a	s	a	l	a	l	o	m	a	e	s	t	e				
T. cifrado	K	M	W	G	W	L	B	V	Z	D	H	A	E	T	O	S	W	Q	L	S	Z	B	I				

La cadena de encriptación que comienza con **H**, el alfabeto de codificación 7, es el alfabeto cifrado que se utilizará para encontrar la letra que sustituirá a la **d** del texto llano. Observamos dónde se cruza la columna que comienza por d con la línea que comienza por **H** y resulta ser en la letra **K**. Por consiguiente, a esa letra d del texto llano la representa la **K** en el texto cifrado.
Para codificar la segunda letra del mensaje, **e**, repetimos el proceso. La letra clave que hay sobre la e es la **I**, así que la codificamos mediante un alfabeto diferente del conjunto de alfabetos: la línea que comienza con **I** (el alfabeto de codificación cadena 8), que es un nuevo alfabeto cifrado. Para codificar la e observamos dónde se cruza la columna que empieza por e con la línea que comienza por **I**, y resulta ser en la letra **M**. Por consiguiente, a esa letra e del texto llano la representa la **M** en el texto cifrado. Cada letra de la clave indica un alfabeto cifrado determinado en el conjunto de alfabetos cifrados. La quinta letra del mensaje se codifica según la quinta letra de la clave, **O**, pero para codificar la sexta letra del mensaje tenemos que volver a la primera letra de la clave, **H**. Es decir que para codificar este mensaje se usaron las cadenas 4, 7, 8, 11 y 14. Una palabra clave mas larga incrementaría la complejidad de la cifra.

Se desea que los alumnos de Algoritmos y Programación realicen un programa que permita la codificación o descodificación de mensajes, basándose en el método de codificación o Cifra Vigenère.

El sistema tendrá el siguiente modelo de interfaz:

UCV. Facultad de Ciencias
Escuela de Computación
Algoritmos y Programación
Proyecto 1. La Cifra Vigenère

Menú:
1. Desarrollador
2. Codificar mensaje
3. Decodificar mensaje
4. Salir

Por favor, indique su opción: _____

Opción 1: Debe mostrar el nombre completo, cédula y sección del desarrollador.

Opción 1: Desarrollador

Pedro Pérez
15.145.896
Sección C2

Presione cualquier tecla para volver al menú principal.

Opción 2: Debe solicitar una cadena de texto al usuario y la clave correspondiente para realizar el proceso de codificación, muestra el resultado en Código Vigenère.

Opción 2: Codificar mensaje

Por favor, introduzca el texto a codificar:

DESVIETROPASALALOMAOESTE

Introduzca la clave:

HIELO

La Codificación Vigenére del texto dado es:

KMGWLBVZDHATOSWQLSZBI

Presione cualquier tecla para volver al menú principal.

Opción 3: debe solicitar un Código Vigenère al usuario, y debe realizar el proceso inverso de codificación, para mostrar el resultado como texto normal.

Opción 3: Decodificar mensaje

Por favor, introduzca la codificación:

KMGWLBVZDHATOSWQLSZBI

Introduzca la clave: HIELO

El texto correspondiente es:

DESVIETROPASALALOMAOESTE

Presione cualquier tecla para volver al menú principal.

Opción 4: permite salir del programa.

TODO PROYECTO DEBE INCLUIR (EN UN SOBRE IDENTIFICADO Y CERRADO):

- Un informe escrito (impreso) contentivo de: Análisis detallado del problema, con la explicación en **lenguaje natural**, máximo 3 páginas, sobre cuál es el problema planteado y la solución propuesta (**no transcribir el enunciado**).
- Algoritmo en notación pseudoformal, que refleje la solución.
- Listado del programa en Java, DOCUMENTADO.
- Entregar los documentos IMPRESOS y el código fuente documentado del programa en CD o CD Regrabable y libre de virus.
- Cada material debe ser identificado y debe ser entregado dentro de un sobre identificado y cerrado. **Sobre sin la debida identificación, proyecto que NO SE CORRIGE**.

RESTRICCIONES DEL PROYECTO:

- Debe ser realizado individualmente, en lenguaje Java y sobre entorno Linux o Windows.
- Se deben realizar las validaciones respectivas para el correcto funcionamiento del programa.

- Sólo se deben usar las herramientas algorítmicas vistas en clase, hasta ciclos.

- Cualquier duda con el entorno de programación para Java o con el enunciado del proyecto, no dude en plantearla a su preparador.

- Cualquier otra restricción será o aclaratoria del proyecto será publicada en la página de la materia, así que deben estar pendientes de estar revisando esta página.

ENTREGA **Lunes, 10 de Noviembre de 2008**, en salones y horas de clase de teoría (3pm a 5pm).

Éxito, GDAyP, 02 de Octubre de 2008