Introducción a las Ciencias de la Computación
ENTRADA/SALIDA

1 Objetivo

En esta práctica vamos a implementar el método clásico de cifrado Vigeniere para llevar a cabo una comunicación confidencial, utilizando para ello lectura y escritura de archivos.

2 Desarrollo

El cifrador de Vigenere

Se le denominó así en honor al francés Blaise de Vigenere. Este cifrado consiste en lo siguiente: se crea una matriz de 26 x 26 y se rellena escribiendo en cada fila un alfabeto que se irá desplazando a la izquierda de uno en uno, e identificamos a cada fila y columna con una letra:

	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
Fila A	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
Fila B	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
Fila C	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
Fila D	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
Fila E	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
Fila F	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
Fila G	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
Fila H	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
Fila I	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
Fila J	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
Fila K	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
Fila L	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
Fila M	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
Fila N	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
Fila O	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
Fila P	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
Fila Q	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
Fila R	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
Fila S	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
Fila T	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
Fila U	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
Fila V	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
Fila W	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
Fila X	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
Fila Y	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
Fila Z	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

Después se decide una palabra clave y se va repitiendo ininterrumpidamente, de forma que el texto a cifrar y la palabra clave tengan la misma longitud. Por ejemplo, con el texto plano "ESTO ES UN SECRETO" y la clave "PUERTA" quedaría representado de este modo:

ESTOESUNSECRETO
PUERTAPUERTAPUE

Para cifrar el texto utilizando la Tabla de Vigenere se procede de la siguiente manera:
Nos posicionamos en la columna que pertenezca al texto y en la fila que pertenezca a la clave y el elemento que contenga dicha intersección será la letra que cifre dicho par.
Por ejemplo la letra P cifrada con la clave E nos daría el criptograma T. Siguiendo esto como ejemplo nuestro texto plano cifrado quedaría representado de este modo:

TMXFXSJHWVVRTNS

Para descifrar un mensaje, es necesario volver a pedir la llave y completarla al tamaño del texto. Por ejemplo:

TMXFXSJHWVVRTNS
PUE RTAPUERTAPUE

Posteriormente ir al renglón de la palabra clave, y buscar la letra del texto cifrado; la columna será el resultado. En nuestro caso tenemos que ir al renglón P y buscar la letra T, a la cual le corresponde la columna E.

3 Ejercicios

Completa la clase **Vigeniere** que será la responsable de cifrar o descifrar un mensaje y **Main** la cual desplegará un menú que muestra las opciones cifrar o descifrar un archivo. Posteriormente, pide la ruta absoluta de un archivo en donde se encuentra el texto plano o el texto cifrado y finalmente solicita la clave. El programa debe de escribir un archivo, ya sea con el texto cifrado o descifrado según sea el caso.
NOTA1: Para cifrar utiliza archivos con extension .**encoded**, que en realidad será un txt para proporcionar el texto plano. El programa debe producir un archivo en la misma ruta pero con extensión .**decoded.** El caso contrario aplica cuando se descifra un archivo.
NOTA 2: Los caracteres que no esten entre a-z deben quedar sin modificación.

Un caso de prueba:
UWA JKGV NQ TQIZCUBG! AI ECAK VMTOQPCA GN KWTAQ FM KEK.
SECRETO: icc