TEMA 6: **DISEÑO DE CLASES**

PROBLEMA 4. **EL CÓDIGO DA VINCI**

Actividad 1: **Decodificar mensajes en ficheros de texto**

En el siglo XV, el matemático **León Battista Alberti**, sugirió un método de encriptado de mensajes que dificultaba el uso de información sobre la frecuencia relativa del número de caracteres. El método no se reducía a cambiar caracteres individuales (la "A" por la "J", la "B" por la "R",…) sino que utilizaba dos alfabetos. Veamos un ejemplo.

Siguiendo los alfabetos propuestos en la **Tabla 1**, cifraríamos un mensaje secreto eligiendo de forma alternativa las letras de cada diccionario. Así nuestro mensaje secreto **"ELRESERVADO"** quedaría cifrado como **"KAOFRFSQGVJ"**, al sustituir las letras impares con el **alfabeto 1** y las letras pares con el **alfabeto 2**. Como podemos observar a simple vista, la letra **'E'** de nuestro mensaje original aparece una vez con la forma **'K'** y otras **dos veces** con la forma **'F'**, dificultando el análisis en frecuencia. La letra **'R'** también queda sustituida una vez por la letra **'O'** y otra por la **'S'**, diluyendo así su características estadística.

Alfabeto inicial	**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
Alfabeto cifrado1	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
Alfabeto cifrado2	**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

Tabla 1: Ejemplo de alfabetos para múltiple cifrado de Alberti

Un siglo después, el diplomático **Blaise** de **Vigenere,** basándose en los trabajos de Alberti, crea un método más complejo llamado **"La cifra indescifrable". Vigenere** usaba **26 alfabetos** diferentes para el cifrado, diferenciándose cada uno de ellos en que empezaba una letra más tarde que el anterior, como muestra la **Tabla 2**. La forma de trabajar con la nueva cifra no es complicada, pero es más trabajosa que el tradicional cifrado monoalfabético. Tomando como referencia la tabla de **Vigenere** con los **26 alfabetos**, se elige una palabra como clave secreta, que servirá para elegir el alfabeto que usaremos en cada letra. El alfabeto elegido en cada caso es el que tiene en la primera posición la letra de correspondiente de la palabra clave.

Por ejemplo para codificar la palabra **"ELRESERVADO**", se usa el alfabeto que empieza por cada letra de la palabra clave **"GATOS"**.

Mensaje	E	L	R	E	S	E	R	V	A	D	O
Clave	G	A	T	O	S	G	A	T	O	S	G
Cifrado	K	L	K	S	K	K	R	O	O	V	U

Tabla 2: Ejemplo de alfabetos para el cifrado de Vigenere

Nuestra palabra cifrada entonces pasa a ser "**KLKSKKROOVU"**, palabras para las que el resultado del cifrado no conserva en absoluto las propiedades estadísticas y, la misma letra en el texto de salida puede representar a varias letras diferentes del alfabeto de entrada, como ocurre en nuestro caso con la letra **'K'**, generando una enorme ambigüedad para el criptoanalista.

	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Tabla 2. Tabla de Vigènere para su método **"La cifra indescifrable".**

Se solicita:

- Completar las clases "Codificador" y "Decodificador". Consideraremos que en el fichero solo aparecen letras mayúsculas, número y símbolos de puntuación. Los caracteres que no sean letras no se codificarán, esto es, un punto se codifica como un punto, los espacios en blanco se sustituyen por espacios en blanco, los números por número, etc.
- El contenido de cada fichero (original, codificado y decodificado) debemos poder visualizarlo por pantalla.
- Para codificar o decodificar un archivo se debe emplear la misma clave (solo con letras mayúsculas).
- Los archivos codificados deberán tener añadido al nombre "*codif_*" y los decodificados "*decodif_*". Por ejemplo, si tenemos el archivo "`C:\\prueba\\texto.txt`", el fichero codificado se llamará "`C:\\prueba\\codif_texto.txt`", y si decodificamos este último, se llamará "`C:\\prueba\\decodif_codif_texto.txt`".