

## UF2\_Practica\_06: Creació d'una pàgina de xifratge/desxifrat emprant classes.

### ENUNCIAT

El xifratge Vigenère és un xifratge basat en diferents sèries de caràcters o lletres del xifratge de Cèsar formant aquests caràcters una taula, anomenada taula de Vigenère , que s'usa com a clau. El xifratge de Vigenère és un xifratge polí alfabètic i de substitució.

El xifratge Vigenère s'ha reinventat moltes vegades. El mètode original va ser descrit per Giovan Batista Belas en el seu llibre de 1553 "La xifra del Sig Giovan Batista Belas" . No obstant això, va ser incorrectament atribuït més tard a Blaise de Vigenère, concretament al segle XIX, i per això encara se'l coneix com el "xifratge Vigenère".

Aquest xifratge és conegut perquè és fàcil d'entendre i implementar, a més sembla irresoluble, això el va fer valedor del sobrenom el codi indesxifrabable ( li Chiffre indéchiffrable , en francès).



Aquest tipus de xifrat es basa en una taula, on a la primera fila tenim l'alfabet sencer, i a les línies següents, cap avall, aquest alfabet es desplaça cap l'esquerra, en un caràcter.

Nosaltres hem creat el nostre alfabet per utilitzar-lo tan en català com en castellà. Hem prescindit de la *ela geminada* (L·L), per les dificultats que això pot comportar i la disposició de massa temps per implementar-lo, i més en un control.

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

Haurem de fer el control amb aquesta taula. Fixeu-vos que només hi han majúscules, vocals sense accentuar, sense espais en blanc ni caràcters especials.





El missatge es codifica utilitzant la clau repetida, tantes vegades com calgui, per cadascuna de les lletres del missatge entrant.

**Entrada:** DIVENDRESCONTROLALAUNA

**Clau:** RIUSRIUSRIUSRIUSRIUSRI

**SORTIDA:** VQPXEMMXKKJFLAJDRTUNEI

De tal forma que la clau tingui el mateix nombre de caràcters que el missatge entrant.

## missatge

clau

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

Fixeu-vos en el mecanisme. La primera lletra del missatge, primera fila, la D, i la primera lletra del codi, primera columna, la R, coincideixen, en la taula, amb la V.

D'aquesta manera consecutivament amb tot el missatge. Per descodificar es fa a l'inrevés. Sabent la lletra del missatge codificat i la clau, obtenim el missatge original. Es necessari utilitzar matrius abans que " strings " en el vostre codi, sempre que sigui possible.

### PREMISSES:

- El codi necessari haurà d'estar encapsulat a una classe amb els atributs i mètodes necessaris que permeti fer el xifratge i desxifrat.
- La classe haurà d'estar en un arxiu a part anomenada Vigenere.js
- Des de l'HTML únicament s'haurà de cridar una funció principal que sigui l'encarregada d'instanciar i cridar al mètode necessari.

### LLIURAMENT :

Deseu els fitxers amb el nom UF2-PR06cognom1.zip" i el lliureu a l'aula virtual.

On " cognom1 " correspon al vostre primer cognom. Exemple: Si el vostre cognom fos Ferran Sáez Martínez, l'arxiu el podríeu anomenar UF2-PR06-saez.zip".