La xifra de Vigenère

Tipus	De substitució polialfabètica
Història	Al segle XVI el francès **Blaise de Vigenère** va millorar unes idees un segle anteriors de l'artista-matemàtic italià **Leon Battista Alberti**. Vigenère va publicar un llibre titulat *Traité des chiffres où secrètes manières d'escrire* on explicava una forma de xifratge **polialfabètic**: Una mateixa lletra, al llarg del missatge, pot està representada per altres de forma canviant. Una **A** podrà ser algunes vegades una **D** o una **H**, però, atenció!, no sempre la **D** o la **H** representarà la **A**. En el fons la xifra de Vigenère era una forma d'utilitzar la xifra del Cèsar amb uns quants alfabets a la vegada. Però el mètode era tan bo que el va poder publicar sense guardar-lo en secret perquè encara que al començament del missatge estigués escrit ben clarament "AQUEST MISSATGE ESTÀ XIFRAT AMB EL SISTEMA DE VIGENÈRE" sense la paraula clau era pràcticament impossible descodificar-lo.

Mètode

Per codificar amb la xifra de Vigenère disposem d'una taula amb 26 alfabets.

	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

Després es tria una paraula clau. Per exemple podem triar COL.

A continuació anem escrivint la paraula clau a sota de cada lletra del missatge. Codificarem una "paraula" llarga amb només tres lletres diferents: *cucurrucucú*.

c	**u**	**c**	**u**	**r**	**r**	**u**	**c**	**u**	**c**	**u**
C	O	L	C	O	L	C	O	L	C	O

Només treballarem amb tres dels alfabets de la taula: els que es corresponen amb les lletres de la paraula clau: el C, l'O i el L.

	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**
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
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
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

Codificarem les lletres del missatge que estiguin a sobre de les C de la clau amb l'alfabet C.

c	**u**	**c**	**u**	**r**	**r**	**u**	**c**	**u**	**c**	**u**
C	O	L	C	O	L	C	O	L	C	O
E			**W**			**W**			**E**	

Després les que estiguin aparellades amb l'O amb l'alfabet corresponent i les de la L amb el seu.

c	**u**	**c**	**u**	**r**	**r**	**u**	**c**	**u**	**c**	**u**
C	O	L	C	O	L	C	O	L	C	O
E	**I**	**N**	**W**	**F**	**C**	**W**	**Q**	**F**	**E**	**I**

Si t'hi fixes la lletra c ha quedat codificada amb E i N i Q i la lletra F del codi pot representar una R o una U

Tasques

1) Codifica aquest missatge: "Això no ho entendrà ningú" amb la clau PEIX.

2) Descodifica aquesta paraula amb la mateixa clau: HM YRT IVQTRK XFYMPI GWAX

3) Intercanvia un missatge breu codificat amb una companya o company de la classe. Pots intentar fer-ho per senyes indicant les xifres amb els dits de cada mà.