

## Xifra de Cèsar

<b>Tipus</b>	De substitució monoalfabètica
<b>Història</b>	La va fer servir Juli Cèsar al segle I a.n.e. i encara es s'utilitzava a la Guerra de Secessió nord-americana al segle XIX per tots dos exèrcits enfrontats. La forma d'encriptar d'alguns programes de correu electrònic coneguda com a ROT-13 no és ni més ni menys que una xifra de Cèsar amb 13 desplaçaments.

### Mètode

S'ha de construir un alfabet a partir d'una clau acordada. Per exemple si la clau és **R** a sota de la lletra A s'escriu una R i es segueix per ordre alfabètic. Quan a l'alfabet de codificació s'arriba a la Z es continua a partir de l'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
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

Et pots construir un reglet com aquest per fabricar alfabet de Cèsar:



### Exemple

<b>Text clar</b>	<b>d</b>	<b>i</b>	<b>n</b>	<b>o</b>	<b>s</b>	<b>a</b>	<b>u</b>	<b>r</b>	<b>e</b>
<b>Text codificat</b>	U	Z	E	F	J	R	L	I	V

### Tasques

- 1) Construeix-te un alfabet de Cèsar amb clau **G**.

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

- 2) Codifica aquest missatge am: "Quedem al lloc de sempre"
- 3) Descodifica aquest missatge: SORRUX GR RRUI JK RGRZXK JOG
- 4) Intercanvia un missatge breu codificat amb una companya o company de la classe.

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

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	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
Reglet																																																			