

Si ho amague, ho trobes? Aritmètica del rellotge

M^a Joaquina Berral Yerón, Inmaculada Serrano Gómez

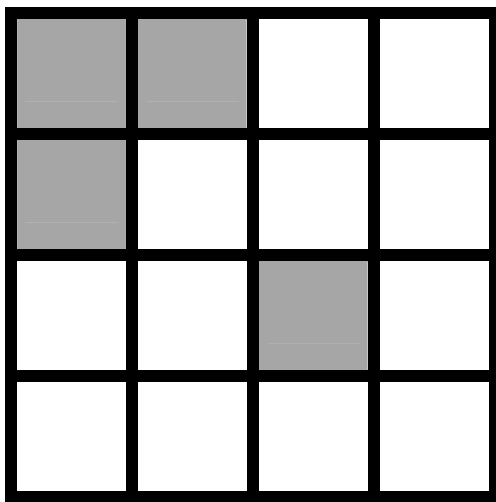


Xifrat amb reixetes o plantilles

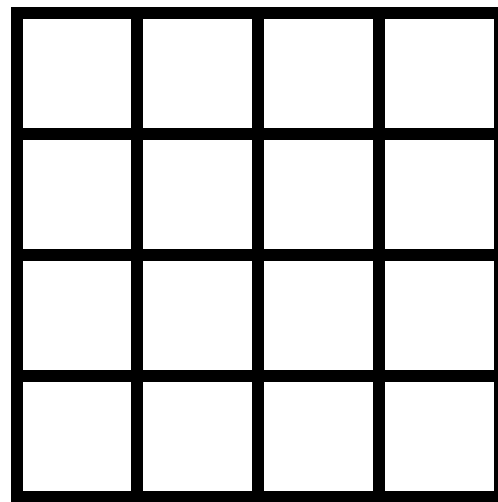
La idea de xifrar usant plantilles amb forats és de Girolamo Cardano, matemàtic italià del segle XVI (que també es considera el precursor del llenguatge braille).

Anem a descobrir aquest mètode de xifrat a poc a poc, per a fer-ho has d'anar realitzant i contestant a les següents preguntes:

Comencem fent la nostra plantilla.



Plantilla A
Els requadres grisos són forats



Quadrícula sense forats

1. Agafa la plantilla A i col·loca-la sobre una quadrícula sin foradar. Marca amb un bolígraf els forats sobre la quadrícula.
2. Gira 90° la plantilla A sobre el seu centre i en sentit horari, deixant fixa la quadrícula de sota i marca en la quadrícula de sota els forats.
3. Torna a fer el mateix, des de la posició actual gira 90°(o 180° la plantilla en posició original) en sentit horari i marca en la quadrícula.
4. Repeteix altra vegada el mateix, és a dir gira 270° la plantilla A en posició original i marca els forats.
5. Retira la plantilla A i observa la quadrícula. S'han marcat els 16 quadrats de la quadrícula una única vegada.
6. ¿Creus que amb qualsevol plantilla de 4x4 i quatre forats passaria el mateix?
7. Realitza una plantilla que verifiqui allò anterior.

Si ho amague, ho trobes? Aritmètica del rellotge

M^a Joaquina Berral Yerón, Inmaculada Serrano Gómez



8. Realitza una plantilla que no ho verifique.

Julio Verne, dedica la novel·la *Matías Sandorff* a Alejandro Dumas, per això agafa com a model el personatge del comte de Montecrist. En aquesta novel·la el comte Sandorf és obligat a adoptar una altra identitat per tal de venjar-se dels seus enemics que raptaren la seva filla.

Una bona part del relat gira en torn a un missatge xifrat. En la novel·la s'explica com el comte i els seus partidaris intenten independitzar Hongria de l'Imperi Austríac. En l'intercanvi d'informació utilitzen un sistema de xifrat de transposició basat en plantilles.

Però, com podem usar una plantilla per xifrar? Segur que ja ho has esbrinat, és molt senzill:

- Pensa en un missatge que com a màxim tinga 16 símbols. En cas de tenir menys, afegeix un poc de soroll, alguna cosa que no distorsione el missatge, per exemple lletres com “w” o “x” que en català apareixen poc.
- Col·loca la teva plantilla en posició original sobre la quadrícula.
- En compte de marcar els forats sobre la quadrícula, agafa les quatre primeres lletres del teu missatge i escriu cadascuna d'elles en un forat, mantenint l'ordre d'escriptura, és a dir reomplint els buits d'esquerra a dreta i de dalt cap a baix.
- Gira la plantilla en sentit horari i escriu en els forats les quatre lletres següents. Repeteix el procés girant l'original 180° i 270°.
- Llegint la quadrícula d'esquerra a dreta i de dalt cap a baix., escriu les teves 16 lletres una darrere de l'altra. Ja tens el missatge xifrat.

Exemple:

Anem a xifrar amb la nostra plantilla el missatge **“hola a tots i bon dia”**

No hem d'afegir soroll perquè té 16 lletres: **“holaatotsibondia”**

h	o		
l			
		a	

Original

		a	t
			o
	t		

Gir 90°

	s		
			i
		b	o

Gir 180°

		n	
d			
i	a		

Gir 270°

h	o	a	t
l	s	n	o
d	t	a	i
i	a	b	o

I el missatge xifrat és ... **“hoatlsnodtaiabo”**

9. Segur que ja saps com desxifrar un missatge rebut i per que ens demostres les teves habilitats

- Agafa la plantilla que has realitzat en el punt 7 d'aquesta activitat

Si ho amague, ho trobes? Aritmètica del rellotge

M^a Joaquina Berral Yerón, Inmaculada Serrano Gómez



- Xifra un missatge i passa'l al teu company/a, enviant-li tot el necessari per què pugui desxifrar-lo. El teu company/a t'enviarà el seu.
 - Desxifra el missatge rebut.
10. Amb una plantilla, es pot xifrar un mateix missatge de diferents formes? Digues almenys tres formes distintes.