La xifra de Rail

Tipus	De transposició
Història	Té el seu origen en la *scytala espartana*, un estri de codificació que es feia servir a l'antiga Grècia. S'escrivia un missatge en un cinta enrotllada amb un bastó de forma que al treure-la les lletres quedaven en un aparent desordre. Per llegir el missatge s'havia d'enrotllar la cinta en un bastó del mateix diàmetre.  A la 1a Guerra Mundial les matrius es feien servir per complicar més la codificació de missatges amb altres alfabets. Per exemple en la *xifra ADFGVX*

Mètode

El mètode més simple es escriure el missatge a una taula amb una amplada acordada, per exemple 5. Després es copien les columnes una a una. Les que quedin buides s'han d'omplir amb signes neutres (per exemple X) . Codifiquem el missatge "Qualsevol nit pot sortir el sol"

Q	U	A	L	S
E	V	O	L	N
I	T	P	O	T
S	O	R	T	I
R	E	L	S	O
L	X	X	X	X

Text codificat: QEISRL UVTOEX AOPRLX LLOTSX SNTIOX

Podem complicar el desordre utilitzant una paraula clau que encapçalaria la taula. Després reordenaríem la taula seguint l'ordre alfabètic de la clau.

Per exemple podem fer servir la clau CALAIX

C	**A**	**L**	**A**	**I**	**X**
Q	U	A	L	S	E
V	O	L	N	I	T
P	O	T	S	O	R
T	I	R	E	L	S
O	L	X	X	X	X

Les lletres de la paraula clau s'ordenen alfabèticament:

CALAIX --- AACILX

A continuació es reordenen les columnes de la taula seguint aquest ordre alfabètic

A	**A**	**C**	**I**	**L**	**X**
U	L	Q	S	A	E
O	N	V	I	L	T
O	S	P	O	T	R
I	E	T	L	R	S
L	X	O	X	X	X

Per acabar es copien les columnes d'esquerra a dreta

Text codificat: UOOIL LNSEX QVPTO SIOLX ETRSX

Tasques

1) Codifica aquest missatge amb la paraula clau MENYS: "Guarda bé aquest secret"

2) Descodifica aquest missatge fet amb la paraula clau CANVI:

OAEOSX NRUCII GQSIMX MDDNDX AAEFEEX

3) Intercanvia un missatge breu codificat amb una companya o company de la classe.