La xifra de Rail

Tipus	De transposició
Història	És un mètode de xifrat molt fàcil d'utilitzar i que es va fer servir, per exemple, a la Guerra de Secessió Nord-americana (1861-1865)

Mètode

Fem primer un exemple amb dues files.

- escrivim el missatge fent servir dues línies i anotant, alternativament, una lletra a cada línia.
- copiem les dues línies consecutivament

Mirem com es codifica el missatge: "Quedem aquesta nit"

Q		E		E	A	U	S	A	I
	U		D	M	Q	E	T	N	T

QEEAUSAI UDMQETNT

Es pot fer també amb tres o més línies. Mirem-ho amb tres

Q			E	A		S		N	
	U	D			Q	E		A	I
		E		M		U	T		T

QEASN UDQEAI EMUTT

Tasques

1) Codifica aquest missatge amb 2 i tres línies: "No li diguis a ningú"

2) Descodifica aquest missatge fet amb 2 línies:

QAEVDSETRLIOARECRHEAUNSAEPRAEDNSUENAAIR

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