La xifra de Playfair

Tipus	De substitució polialfabètica
Història	Va ser creada per Charles Wheatstone i adoptada pel Govern Britànic a l'any 1854

Mètode

1a fase: construir una graella a partir d'una paraula clau

Es fa una graella de 5x5 i s'escriuen primer les lletres, sense repetir, de la paraula clau. Després s'acaba d'omplir la graella alfabèticament amb les lletres que falten. Com que no falta espai per alguna lletra es pot fer una casella doble o bé ometre una lletra. Nosaltres no posarem la W. La paraula clau serà CALAIXERA

C	**A**	**L**	**I**	**X**
E	**R**	**B**	**D**	**F**
G	**H**	**J**	**K**	**M**
N	**O**	**P**	**Q**	**S**
T	**U**	**V**	**Y**	**Z**

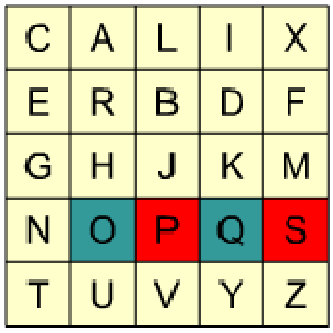
2a fase: preparar el missatge

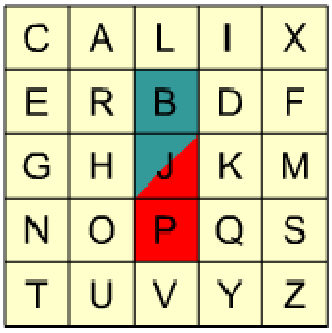
Hem de separar en grups de dos lletres el text del missatge. Si cal completar una parella podem posar una X

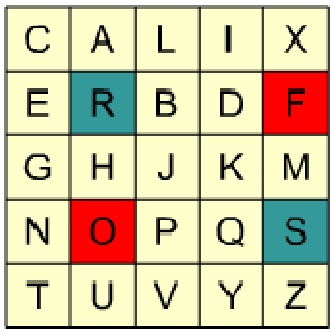
dinosaure	di no sa ur ex

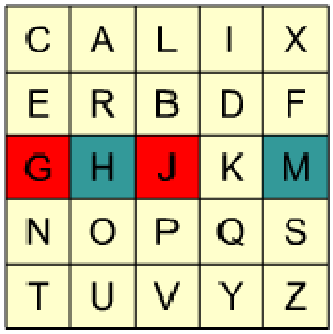
3a fase: codificar segons les regles

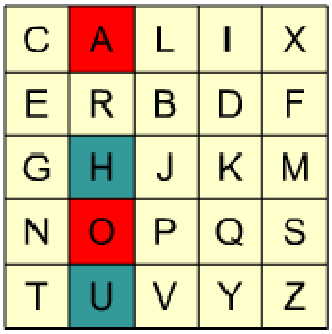
Per codificar cada parell de lletres s'han de buscar a la taula i substituir-les per altres seguint aquestes regles:

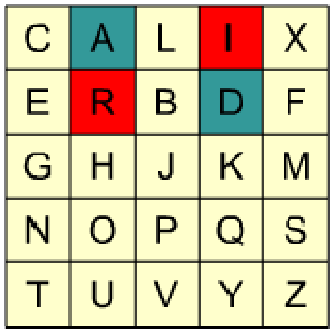
<table>
<tr><th>Regla 1</th><th>Regla 2</th><th>Regla 3</th></tr>
<tr><td>Si les dues lletres de la parella estan a la mateixa línia s'agafen les de la dreta de cadascuna.</td><td>Si estan a la mateixa columna s'agafen les de sota.</td><td rowspan="2">Si estan en línies diferents s'agafen les que "tanquen el rectangle" i cada lletra es canvia per la de la seva fila</td></tr>
<tr><td>Clar: OQ
 

Codificat: PS</td><td>Clar: BJ
 

Codificat: JP</td><td rowspan="2">Clar: RS
 

Codificat: FO</td></tr>
<tr><td>Si una de les lletres és l'última de la fila s'agafa la primera</td><td>Si una de les lletres és la de sota de tot s'agafa la de dalt</td></tr>
<tr><td>Clar: HM
 

Codificat: JG</td><td>Clar: HU
 

Codificat: OA</td><td>Clar: AD
 

Codificat: RI</td></tr>
</table>

DINOSAURE amb la clau CALAIXERA es converteix en **KDOPOXAHFC**.

Tasques

1) Codifica aquesta paraula: “Ratpenat” amb la clau ALBERCOC.

2) Descodifica aquesta paraula amb la mateixa clau: GLPHP GLMUH

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.