1.3 Lesson 2 : Transposition ciphers

■ **Exemple 1.1 — Route Cipher.** Lets encrypt the plaintext "abort the mission, you have been spotted" using 5 columns. We use nulls at the end of the message to make a rectangle.

A	B	O	R	T
T	H	E	M	I
S	S	I	O	N
Y	O	U	H	A
V	E	B	E	E
N	S	P	O	T
T	E	D	X	X

With a route of **reading down the columns** we get the ciphertext "ATSYV NTBHS OESEO EIUBP DRMOH EOXTI NAETX".

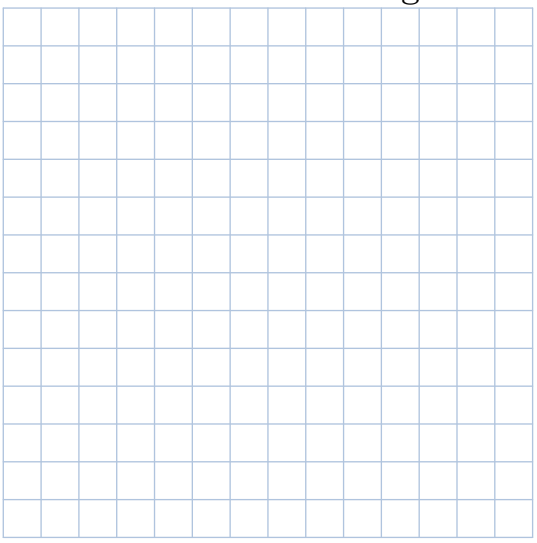
If we chose a route **spiralling inwards counter-clockwise from the bottom right** we get "XTEAN ITROB ATSYV NTEDX OEHOM EHSOE SPBUI".

To decrypt the message, we need to know the route used as well as width or height of the grid.

Exercise 6

You intercept the following message "ASNEF OELBC VYNAW EEEOO NASRN UTIYI EIDMT".

1. How many letters are there? .....
2. What possibilities are there for the shape of the grid?.....
   .....
3. Assume the route used is **reading down the columns**, use the previous information to unscramble the message.



Exercise 7

You intercept another message "TCTES WSGHU ORAAR HESMI LYIT"

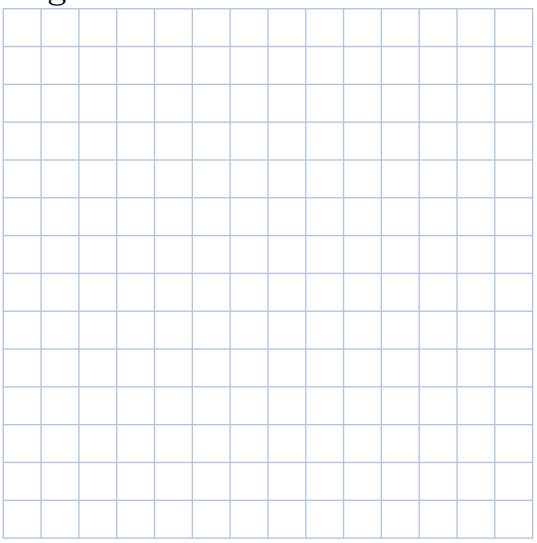
(Note : it is usual to insert a space after every fifth letter, but these spaces should be ignored when finding the size/shape of the grid)

1. Count the letter .....

2. What possibilities are there for the shape of the grid? .....

   .....

3. Thinking about what the first word in the message could be, find the correct shape of the grid and then unscramble the message.



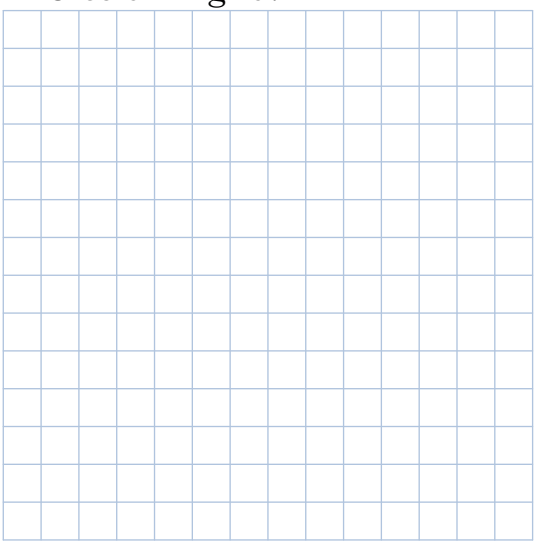
Exercise 8 Suppose you want to scramble the message "A bayonet is a weapon with a worker at each end".

This has 37 letters. The only grids with 37 spaces would have either one row or one column and would not scramble the message. To make it fit a more convenient grid we can add extra **dummy letters** at the end that do not form part of the message, but just fill the space.

1. Consider what happens if you add 1, or 2 dummy letters to the message above. What makes you think these are not good choices? .....

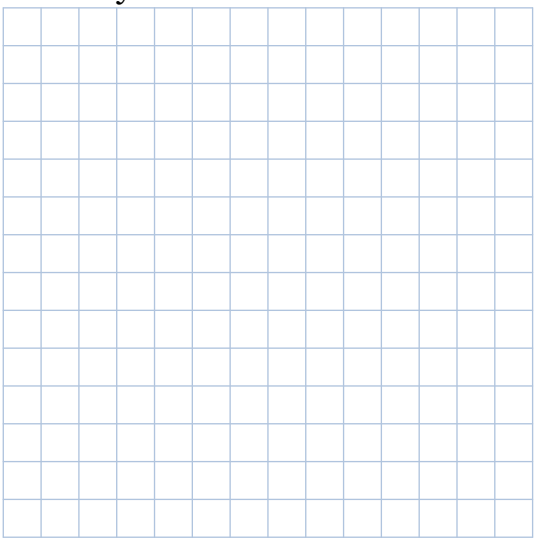
   .....

2. Add three dummy letters X. What is the scrambled message when using an 8-row by 5-column grid.



Exercise 9 One disadvantage of dummy letters is that they give people a clue as to the shape of the grid. Take the scrambled 48 letters message "NDHOA NOOAS BGPSR EOGEO MWUOO MAHTO PUSOD DLCTG OXEHH OIX".

1. Suggest some possible grids to use for scrambling a message with 48 letters.....
   .....
2. Assuming the two Xs near the end of this message are dummy letters, how far apart are they? .....
3. Use your answers to work out the shape of the grid and then unscramble the message.



During the American Civil War (1861-1865), the Confederacy and the Union had to come up with their own new cipher methods as the one previously used were compromised. **Anson Stager** introduced for all telegraph lines used by the North, a simple but effective **word transposition cipher**. The instructions were printed on cards about 3 by 5 inches in size. They included : the **route**, the **keys**, the **code** words and the **null** words.

Exercise 10 — **Work in pairs.** Watch Brian Veitch explains how the North cipher worked.

Discuss the weaknesses and strengths of the Stager cipher used by the North.....
.....
.....
.....
.....
.....

Hints, words to use : jumbled words, train cipher operators, simple key words, guess route used, confusing null words, practicable cipher, delay encription.

Exercise 11 This cipher message was sent to Major General George McClellan on April 1861:

> "*Telegraph* the have be not I hands profane right hired held must start my cowardly to an responsible Crittenden to at polite ascertain engine for Colonel desiring curse demands the to success by not reputation nasty state go of superseded Crittenden past kind of up this being Colonel my just the road division since advance sir kill ."

The **code word** *Telegraph* meant that this cipher message is read row by row from a grid eight lines long, with seven columns.

1. Write down (row by row) the cipher text in 8 rows of 7 columns each.

2. The **code word** *Telegraph* meant also that the plaintext was inserted in the order : *up the 6th column, down the 1st, up the 5th column, down the 2nd, up the 4th, and down the 3rd. The 7th column is filled with nulls.* Write down the plain message : .....

.....

.....