11 Transposition

One method of encrypting messages is called *transposition.* A message, for example,

THIS IS A MESSAGE. HI.

is written across the rows in a grid:

T	H	I	S
I	S	A	M
E	S	S	A
G	E	H	I

To obtain the encrypted message, simply read down the columns:

TIEGHSSEIASHSMAI

To decrypt the message, do the reverse: write down the columns and read across the rows,

The security of this system lies in having to know the size and shape of the grid.

Example 1

You intercept the following message

ASNEFOELBCVYNAWEEEOONASRNUTIYIEIDMT

a) How many letters are there?

b) What possibilities are there for the shape of the grid?

c) Use the information from (a) and (b) to unscramble the message.

Solution

a) 35 letters

b) 5 rows by 7 columns or 7 rows by 5 columns

c) 7 rows by 5 columns gives the grid:

A	L	W	A	Y
S	B	E	S	I
N	C	E	R	E
E	V	E	N	I
F	Y	O	U	D
O	N	O	T	M
E	A	N	I	T

Reading along the rows, the message is

'ALWAYS BE SINCERE EVEN IF
YOU DO NOT MEAN IT'

Exercise 1

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.*)

a) *Count the letters.*

b) *What possibilities are there for the shape of the grid?*

c) *Find the correct shape for the grid and then unscramble the message.*

Suppose you wanted 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. *Why not*?

37 is an example of a prime number, a number that is not divisible by any number other than itself or one. To make it fit a more convenient grid we can add extra letters at the end that do not form part of the message, but just fill the space. It is common to use 'unusual' letters, for example, X. Such letters are commonly known as *dummy* letters.

Activity 1

Consider what happens if you add a) 1, b) 2 dummy letters in the message above.

What makes you think that these are not good choices?

If we add three dummy letters, we have 40 letters, which gives us many more choices (e.g. 4 by 10, 8 by 5, etc.).

We are going to use an 8-row by 5-column grid:

A	B	A	Y	O
N	E	T	I	S
A	W	E	A	P
O	N	W	I	T
H	A	W	O	R
K	E	R	A	T
E	A	C	H	E
N	D	X	X	X

So the scrambled message is:

ANAOH KENBE WNAEA DATEW WRCXY IAIOA HXOSP TRTEX

One disadvantage of dummy letters is that they give people a clue as to the shape of the grid. The next example shows how.

Example 2

The message

NDHOA NOOAS BGPSR EOGEO MWUOO MAHTO PUSOD DLCTG OXEHH OIX

has 48 letters.

a) Suggest some possible grids to use for scrambling a message with 48 letters.

b) Assuming the two Xs near the end of this message are dummy letters, how far apart are they?

c) Use your answers to a) and b) to work out the shape of the grid and then unscramble the message.

Solution

a) Possible grids :

2 R by 24 C
3 R by 16 C
4R by 12 C
6 R by 8 C
8 R by 6 C
12 R by 4 C
16 R by 3 C
24 R by 2 C

b) 6 letters apart

c) We will try 8 C by 6 R, which gives:

N	O	P	E	O	P	L	E
D	O	S	O	M	U	C	H
H	A	R	M	A	S	T	H
O	S	E	W	H	O	G	O
A	B	O	U	T	D	O	I
N	G	G	O	O	D	X	X

The message is

'NO PEOPLE DO SO MUCH HARM AS THOSE
WHO GO ABOUT DOING GOOD'

Exercise 2

Decode the message

BKDLITESOTOMCPOHERLNRENOYOWPWXAAXRNX

To make the unscrambling process a little trickier, we can read down our columns in a different order than just first, second, third ...

We scramble the message

A NAME MADE GREAT IS A NAME DESTROYED *(30 letters)*

in a 5 row by 6 column grid and read the columns in the order indicated by the numbers above them.

3	***5***	***6***	***4***	***2***	***1***

The message is

MENSD ERAEE AAAAT MGSDY NDTMR AEIEO

In order to unscramble the message we would need to know (or work out) the shape of the grid and the sequence in which to write the columns, 3 5 6 4 2 1. This is an example of a *key*.

Example 3

The scrambled message

ANTHT WVAXE HOSRG HCXIN GAEHI ENWTT AANLO EFTSY YILTG WISTE SAHX

has 54 letters.

What is the message?

Solution

The Xs are all dummy letters and the grid is known to be 9 rows by 6 columns. Even if we didn't know this, we could make a guess at it by looking at how far apart the dummy letters are in the scrambled message. The first X is letter number 9, and the second is letter number 18. The third is letter 54, so all Xs occur at a multiple of 9. So 9 is a very good candidate for the number of rows. (3 is also a possibility, but at least we have got rid of some of the possibilities, 2, 6 and 18.)

Changing the spacing in the message to put a space after each column gives

ANTHTWVAX EHOSRGHCX INGAEHIEN WTTAALOE FTSYYIL TG WISTESAHX

There are three columns that end in X – we would expect these to be the three rightmost columns, and the others would be on the left. So the first three columns (in no particular order) are INGAEHIEN WTTAANLOE FTSYYILTG and the last three (again, in no particular order) are ANTHTWVAX EHOSRGHCX WISTESAHX

From this we see the first three letters of the message are

FIW, FWI, IFW, IWF, WFI or WIF

Exercise 3

a) *Looking at the Example above, which of the alternatives given for the first three letters of the message is most likely?*

b) *Do the same for the other three columns and unscramble the message.*

Activity 2

EREAO ELUOT PXEAH HTTHH TTEII SNIOX NEYVB XGBDE EXTSY OML

Unscramble the message.

Activity 3

Use the transposition method to scramble a message and see if a friend can unscramble it.

Do this again, but this time with a key for the sequence in which to write the columns.