## UNIT 11 Transposition Lesson Plan 1

### Activity 1

#### Introduction

T: We are going to look at another method of coding messages; scrambling them by rearranging the letters. The method is called 'transposition' as the letters are transposed or moved. Do you have any ideas as to how we can do this?

T: One method is to use a grid to reorder the letters. Look at the message on the OS. How many letters are there? (16)

T: What size grid could we use? (4×4 or 8×2 or 2×8)

T: We'll use a 4×4 grid and write the message horizontally in rows from left to right, but we'll read it vertically. Who would like to do this on the board?

P1: T H I S
    I S A M
    E S S A
    G E H I

T: Rewrite the message, working vertically in columns. Another volunteer? ...

P2: T I E G H S S E I A S H S M A I

T: What does the message receiver need to have to unscramble this message? (The grid size)

T: Is this easy? How many possibilities are there? (Just three)

#### Unscrambling

T: I'll give you 4 minutes to work out the message which has been scrambled here.

T: Let's look at your answers.

T: How many letters are there? (35)

T: What are the possible grid sizes? (5×7 or 7×5)

T: Answer? (ALWAYS BE SINCERE EVEN IF YOU DO NOT MEAN IT)

T: Well done! Was it easy to unscramble? (Yes)

T: Why was it easy? (Because there were only two possibilities)

### Activity 2

#### Dummy letters

T: Here is another message to unscramble:

A BAYONET IS A WEAPON WITH A WORKER AT EACH END

T: How many letters are there? (37)

T: What are the possible grid sizes? (1×37 or 37×1)

(continued)

### Notes

Whole class interactive discussion on the problems of coding messages and their security. T can use OS 11.1 or own previously-prepared board.

Class discusses Ps’ suggestions before T introduces the grid approach.

T accepts the alternatives, and possibly follows through the method.

T chooses different volunteer Ps to complete grid on OS/board and to rewrite the message.

T asks all Ps.

Whole class discuss security aspects; T reinforces the concept by letting Ps work through an exercise.

T gives each P a copy of OS 11.2. Ps work in pairs for 5 minutes; T monitors progress, intervening if necessary.

Interactive review of the process involved, with Ps giving answers verbally.

T shows either OS 11.3 or previously-prepared board.
UNIT 11 Transposition Lesson Plan 1

### Codes and Ciphers

**Activity 3 (continued)**

T: What does that not do? *(It doesn't scramble the message)*
T: So why doesn't 37 work? *(It's a prime number)*
T: How can we make it work? *(Add extra letters?)*
T: Yes, we add what are called 'dummy' letters, normally extra Xs.
T: How many should we add? *(1, 2, 3)*

T: We'll use a grid of 8 rows by 5 columns. Who can show this on the board?

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A</th>
<th>Y</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>E</td>
<td>T</td>
<td>I</td>
<td>S</td>
</tr>
<tr>
<td>A</td>
<td>W</td>
<td>E</td>
<td>A</td>
<td>P</td>
</tr>
<tr>
<td>O</td>
<td>N</td>
<td>W</td>
<td>I</td>
<td>T</td>
</tr>
<tr>
<td>H</td>
<td>A</td>
<td>W</td>
<td>O</td>
<td>R</td>
</tr>
<tr>
<td>K</td>
<td>E</td>
<td>R</td>
<td>A</td>
<td>T</td>
</tr>
<tr>
<td>E</td>
<td>A</td>
<td>C</td>
<td>H</td>
<td>E</td>
</tr>
<tr>
<td>N</td>
<td>D</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

T: We need someone else to write out the scrambled message. Write the letters in groups of five.

P₄: The message is

**ANOH KENBE WNAEA DATEW WRXY AIIOA HXOSP TRTEX**

T: Well done.

25 mins

4 Unscrambling

T: Here is an example for you to unscramble. See what you can do!

**NDHOA NOOAS BGPSR EOGEO MWUOO MAHTO PUSOD DLCTG OXEH OIX**

T: What grids could you use? *(2 × 24, 3 × 16, 4 × 12, 6 × 8, 8 × 6, 12 × 4, 16 × 3, 24 × 2)*
T: What else could we look at that will help us? *(The frequency of Xs at the end of the message)*
T: How far apart are they? *(6)*
T: So which of the grids should we try? *(8 × 6)*
T: What is the message? *(NO PEOPLE DO SO MUCH HARM AS THOSE WHO GO ABOUT DOING GOOD)*
T: Good.

35 mins

### Notes

Some discussion on prime numbers may be needed at this stage. T should use Ps ideas if at all possible when covering this.
T should choose (reluctant) Ps to answer.
Whole class discussion on the implications of adding 1, 2 or 3. Conclude that 3 is best as it gives more possibilities for grids.

T chooses another P to write the message on the board.

Discussion as to how best to display the message.

Each P has a copy of the message; T does not initially present the prompt questions. Ps work individually or in pairs.
T intervenes after 4 or 5 minutes to monitor progress and encourages Ps to discuss their strategies.

Ps continue working on the problem for a few more minutes. Then T asks who has an answer and checks that all have understood the method.
### Codes and Ciphers

#### Activity 5

**UNIT 11 Transposition** Lesson Plan 1

**Using a key**

T: Was the last exercise easy to unscramble? **(Yes)**

T: How could we make it more difficult? **(?)**

T: One way is to mix up the order of the columns when completing the grid by using a prescribed KEY that is known to the message receiver.

T: Here is a message which we are going to code using a grid:

<table>
<thead>
<tr>
<th>A</th>
<th>N</th>
<th>A</th>
<th>M</th>
<th>E</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>D</td>
<td>E</td>
<td>G</td>
<td>R</td>
<td>E</td>
</tr>
<tr>
<td>A</td>
<td>T</td>
<td>I</td>
<td>S</td>
<td>A</td>
<td>N</td>
</tr>
<tr>
<td>A</td>
<td>M</td>
<td>E</td>
<td>D</td>
<td>E</td>
<td>S</td>
</tr>
<tr>
<td>T</td>
<td>R</td>
<td>O</td>
<td>Y</td>
<td>E</td>
<td>D</td>
</tr>
</tbody>
</table>

T: The key is

| 3 | 5 | 6 | 4 | 2 | 1 |

T: How many letters are there in the message? **(30)**

T: What is the grid size? **(5 R by 6 C)**

T: We first write out the message in the grid in the usual way.

<table>
<thead>
<tr>
<th>3</th>
<th>5</th>
<th>6</th>
<th>4</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>N</td>
<td>A</td>
<td>M</td>
<td>E</td>
<td>M</td>
</tr>
<tr>
<td>A</td>
<td>D</td>
<td>E</td>
<td>G</td>
<td>R</td>
<td>E</td>
</tr>
<tr>
<td>A</td>
<td>T</td>
<td>I</td>
<td>S</td>
<td>A</td>
<td>N</td>
</tr>
<tr>
<td>A</td>
<td>M</td>
<td>E</td>
<td>D</td>
<td>E</td>
<td>S</td>
</tr>
<tr>
<td>T</td>
<td>R</td>
<td>O</td>
<td>Y</td>
<td>E</td>
<td>D</td>
</tr>
</tbody>
</table>

T: The key means that we take the last column, column 6, first, and continue according to the order given.

Now you complete this!

<table>
<thead>
<tr>
<th>M</th>
<th>E</th>
<th>N</th>
<th>S</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>G</td>
<td>S</td>
<td>D</td>
<td>Y</td>
</tr>
</tbody>
</table>

T: The next problem is to find out how we unscramble a message when a key has been used.

---

**Homework**

Unscramble the message (Example 3 in Pupil Text):

ANTHT WVAXE HOSRG HCXIN GAELI ENWTT
AANLO EFTSY YILTG WISTE SAHX

---

**Notes**

T stresses that the person receiving the message must be given information secretly beforehand to help them unscramble any messages.

T shows OS 11.4 and a copy is given to each pair of Ps.

Each pair of Ps completes their grid.

Ps write out their scrambled message. Volunteer quickly writes theirs on OS on OHP. Other Ps agree or correct this P as they work at board. T monitors Ps' work to check that they have understood.