Codes and Ciphers	**UNIT 11** *Transposition* Lesson Plan 1

Activity		Notes
1	**Introduction**	Whole class interactive discussion on the problems of coding messages and their security. T can use **OS 11.1** or own previously-prepared board.
	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?	
		Class discusses Ps' suggestions before T introduces the grid approach.
	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 accepts the alternatives, and possibly follows through the method.
	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?	T chooses different volunteer Ps to complete grid on OS/board and to rewrite the message.
	P₁:	

$$\begin{array}{|c|c|c|c|} \hline T & H & I & S \\ \hline I & S & A & M \\ \hline E & S & S & A \\ \hline G & E & H & I \\ \hline \end{array}$$

Activity		Notes
	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 asks all Ps.
	T: Is this easy? How many possibilities are there? *(Just three)*	Whole class discuss security aspects; T reinforces the concept by letting Ps work through an exercise.
	10 mins	
2	**Unscrambling**	T gives each P a copy of **OS 11.2**. Ps work in pairs for 5 minutes; T monitors progress, intervening if necessary.
	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)*	Interactive review of the process involved, with Ps giving answers verbally.
	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)*	
	15 mins	
3	**Dummy letters**	T shows either **OS 11.3** or previously-prepared board.
	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)*	
(continued)	T: What are the possible grid sizes? *(1×37 or 37×1)*	

Codes and Ciphers	**UNIT 11** *Transposition* Lesson Plan 1	

Activity		Notes

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?

P₃ (on board):

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

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

P₄: The message is

> ANAOH KENBE WNAEA
> DATEW WRCXY IAIOA
> HXOSP TRTEX

T: Well done.

Notes (right column):

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.

———— *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 OXEHH 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.

Notes (right column):

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.

———— *35 mins* ————

Codes and Ciphers	**UNIT 11** *Transposition* Lesson Plan 1	

Activity		*Notes*
5	**Using a key**	
	T: Was the last exercise easy to unscramble? *(Yes)*	T stresses that the person receiving the message must be given information secretly beforehand to help them unscramble any messages.
	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:	
	A NAME MADE GREAT IS A NAME DESTROYED	T shows **OS 11.4** and a copy is given to each pair of Ps.
	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.	
	Key ③ ⑤ ⑥ ④ ② ①	Each pair of Ps completes their grid.

3	5	6	4	2	1
A	N	A	M	E	M
A	D	E	G	R	E
A	T	I	S	A	N
A	M	E	D	E	S
T	R	O	Y	E	D

	T: The key means that we take the last column, column 6, first,	
	M E N S D	
	and continue according to the order given.	
	Now you complete this!	
	M E N S D E R A E E A A A A T M G S D Y N D T M R A E I E O	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.
	T: The next problem is to find out how we unscramble a message when a key has been used.	
	45 mins	
	Homework	
	Unscramble the message (Example 3 in Pupil Text):	
	ANTHT WVAXE HOSRG HCXIN GAEHI ENWTT AANLO EFTSY YILTG WISTE SAHX	