Codes and Ciphers

UNIT 12 *One-Time Pads* Lesson Plan 1

Activity		*Notes*
		T: Teacher P: Pupil Ex.B: Exercise Book
1	**Introduction**	
	T: This is another cipher that is dependent on the receiver having a key to help decipher the message.	Whole class discussion on different types of codes.
	T: Our first task is to code all letters. To keep it simple we'll code A as 1, B as 2, etc. Note that Z is coded as zero.	T shows **OS 12.1** (or writes on board); each P has a copy of OS.

A	B	C	...	...	...	...	...	X	Y	Z
↓	↓	↓						↓	↓	↓
1	2	3						24	25	0

T: All the arithmetic we use here is 'modulo 26', i.e. remainder on division by 26. So $16 + 11 = 27 = 1 \pmod{26}$, $11 \times 5 = 55 = 3 \pmod{26}$	Class might need further help here; T could use 'modulo 4' as an initial example.
T: What about $17 + 17 = ? \pmod{26}$ *(8)* $11 - 16 = ? \pmod{26}$ *(?)*	T chooses Ps to answer the questions – checks that all understand.
T: For negative numbers we follow the same rule, so that $11 - 16 = -5$ $= -5 + 26 \pmod{26}$ $= 21 \pmod{26}$	T stresses that the answer must be from 0 to 25 but that you can add any positive factor of 26.
T: What about $7 - 14 = ? \pmod{26}$ *(19)*	More examples might be needed to enforce this concept.
T: Now the important concept; a one-time pad (the key) is a collection of random letters. Let's use our one-time pad F X I P U F to code or encrypt the message S E C R E T The method is shown on the slide.	**OS 12.2** is shown to help Ps understand the method.
T: We add together the message and the one-time pad. Who would like to complete this sheet?	Ps (chosen by T) write on board in turn, helped by other Ps if they are struggling.

P (on OS):

	S	E	C	R	E	T			19	5	3	18	5	20
+	F	X	I	P	U	F	⇒	+	6	24	9	16	21	6
	Y	C	L	H	Z	Z	⇐		25	3	12	8	0	0

The coded message is YCLHZ Z

T: Well done. You have to concentrate, but the method is quite straightforward.

T: To decrypt messages we subtract the (one-time pad) key from the coded message. Who would like to show us?

P (on OS):

	Y	C	L	H	Z	Z			25	3	12	8	0	0
–	F	X	I	P	U	F	⇒	–	6	24	9	16	21	6
	S	E	C	R	E	T	⇐		19	5	3	18	5	20

Further discussion might be needed for T to check that all Ps have understood the concept.

T: Good. This is called the additive key method. It is easy to encrypt and decrypt messages if you have the key.

20 mins

Codes and Ciphers	**UNIT 12** *One-Time Pads* Lesson Plan 1	
Activity		***Notes***
2	**Exercises** T: Now try Exercise 1 in your text.	Ps work in pairs for about 5 minutes, writing in their Ex.Bs.; T monitors their work, intervening if necessary.
	T: Who has the answers? Come and write them on the board. P_1 (writing on board): DSNA PFO JLW KI T: To help with security, we usually put the message into groups of 5 letters. Can someone quickly do that for us now? P_2 (on board): DSNAP FOJLW KI T: And for part b) ? Remember to arrange the letters in groups of 5. P_3 (on board): AOPLC JSANN PQSFG T: Well done!	Volunteer Ps write their answers on board; other Ps agree/disagree. Ps write correct answers in their Ex.Bs. Discussion on arrangement of letters in 5s (i.e. it is better not to give any hints as to the spacing of the letters to make words).
	30 mins	
3	**Subtractive key** T: You can also use the subtractive key method; here you <u>subtract</u> the key from the message. T: Who would like to encrypt the message on the OS? P_4 (on OS): S E C R E T ⇒ 19 5 3 18 5 20 – F X I P U F + 6 24 9 16 21 6 Y C L H Z Z ⇐ 13 7 20 2 10 14 T: Very good. T: How can you decipher the message? *(Add the key)* T: Come and show us. P_5 (on OS): M G T B J N ⇒ 13 7 20 2 10 14 + F X I P U F + 6 24 9 16 21 6 S E C R E T ⇐ 19 5 3 18 5 20 T: Well done!	**OS 12.3** on OHP or similar on OS. Volunteer Ps write answers; other Ps agree/disagree. Ps write correct answers in their Ex.Bs.
	35 mins	
4 *(continued)*	**Activity** T: Now we'll look at a third method, called 'minuend'. I'll give you 5 minutes to work through Activity 1. T: Who is going to show us how this method works for encrypting? P (at board): F X I P U F ⇒ 6 24 9 16 21 6 – S E C R E T – 19 5 3 18 5 20 M S F X R L ⇐ 13 19 6 24 16 12	Each pair of Ps is given a copy of Activity 1. They have 5-6 minutes to work on this before T stops them for an interactive review.

Codes and Ciphers	**UNIT 12** *One-Time Pads* Lesson Plan 1	
Activity **4** *(continued)*	T: Good. Who has decrypted the message? P (on board): F X I P U F ⇒ 6 24 9 16 21 6 – M S F X R L – 13 19 6 24 16 12 S E C R E T ⇐ 19 5 3 18 5 20 T: What is the main problem with these methods of coding and can it be overcome? *(Distribution and security of the key)* *45 mins*	***Notes*** T can point out that minuend key is popular as the same operation (subtracting from the key) is used for both encrypting and decrypting. Whole class discussion of how the key is distributed and kept safe, etc.
	Homework Exercise 3 for reinforcement or Activity 2 for creativity	