

<p><i>Codes and Ciphers</i></p>	<p><b>UNIT 12 One-Time Pads Lesson Plan 1</b></p>																																																																																																															
<p><b>Activity</b></p> <p><b>1</b></p>	<p><b>Introduction</b></p>	<p><b>Notes</b></p>																																																																																																														
	<p>T: This is another cipher that is dependent on the receiver having a key to help decipher the message.</p> <p>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.</p> <table border="1" data-bbox="338 524 791 640" style="margin-left: auto; margin-right: auto;"> <tr> <td>A</td><td>B</td><td>C</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>X</td><td>Y</td><td>Z</td> </tr> <tr> <td>↓</td><td>↓</td><td>↓</td><td></td><td></td><td></td><td></td><td></td><td>↓</td><td>↓</td><td>↓</td> </tr> <tr> <td>1</td><td>2</td><td>3</td><td></td><td></td><td></td><td></td><td></td><td>24</td><td>25</td><td>0</td> </tr> </table> <p>T: All the arithmetic we use here is 'modulo 26', i.e. remainder on division by 26. So</p> $16 + 11 = 27 = 1 \pmod{26},$ $11 \times 5 = 55 = 3 \pmod{26}$ <p>T: What about</p> $17 + 17 = ? \pmod{26} \quad (8)$ $11 - 16 = ? \pmod{26} \quad (?)$ <p>T: For negative numbers we follow the same rule, so that</p> $11 - 16 = -5$ $= -5 + 26 \pmod{26}$ $= 21 \pmod{26}$ <p>T: What about</p> $7 - 14 = ? \pmod{26} \quad (19)$ <p>T: Now the important concept; a one-time pad (the key) is a collection of random letters. Let's use our one-time pad</p> <p style="margin-left: 40px;">F X I P U F</p> <p style="margin-left: 40px;">to code or encrypt the message</p> <p style="margin-left: 40px;">S E C R E T</p> <p style="margin-left: 40px;">The method is shown on the slide.</p> <p>T: We add together the message and the one-time pad. Who would like to complete this sheet?</p> <p>P (on OS):</p> <table border="1" data-bbox="344 1505 975 1644" style="margin-left: auto; margin-right: auto;"> <tr> <td>S</td><td>E</td><td>C</td><td>R</td><td>E</td><td>T</td><td></td><td>19</td><td>5</td><td>3</td><td>18</td><td>5</td><td>20</td> </tr> <tr> <td>+ F</td><td>X</td><td>I</td><td>P</td><td>U</td><td>F</td><td>⇒</td><td>+ 6</td><td>24</td><td>9</td><td>16</td><td>21</td><td>6</td> </tr> <tr> <td><u>Y</u></td><td><u>C</u></td><td><u>L</u></td><td><u>H</u></td><td><u>Z</u></td><td><u>Z</u></td><td>⇐</td><td><u>25</u></td><td><u>3</u></td><td><u>12</u></td><td><u>8</u></td><td><u>0</u></td><td><u>0</u></td> </tr> </table> <p style="margin-left: 40px;">The coded message is YCLHZ Z</p> <p>T: Well done. You have to concentrate, but the method is quite straightforward.</p> <p>T: To decrypt messages we subtract the (one-time pad) key from the coded message. Who would like to show us?</p> <p>P (on OS):</p> <table border="1" data-bbox="344 1879 975 2018" style="margin-left: auto; margin-right: auto;"> <tr> <td>Y</td><td>C</td><td>L</td><td>H</td><td>Z</td><td>Z</td><td></td><td>25</td><td>3</td><td>12</td><td>8</td><td>0</td><td>0</td> </tr> <tr> <td>- F</td><td>X</td><td>I</td><td>P</td><td>U</td><td>F</td><td>⇒</td><td>- 6</td><td>24</td><td>9</td><td>16</td><td>21</td><td>6</td> </tr> <tr> <td><u>S</u></td><td><u>E</u></td><td><u>C</u></td><td><u>R</u></td><td><u>E</u></td><td><u>T</u></td><td>⇐</td><td><u>19</u></td><td><u>5</u></td><td><u>3</u></td><td><u>18</u></td><td><u>5</u></td><td><u>20</u></td> </tr> </table> <p>T: Good. This is called the additive key method. It is easy to encrypt and decrypt messages if you have the key.</p>	A	B	C	...	...	...	...	...	X	Y	Z	↓	↓	↓						↓	↓	↓	1	2	3						24	25	0	S	E	C	R	E	T		19	5	3	18	5	20	+ F	X	I	P	U	F	⇒	+ 6	24	9	16	21	6	<u>Y</u>	<u>C</u>	<u>L</u>	<u>H</u>	<u>Z</u>	<u>Z</u>	⇐	<u>25</u>	<u>3</u>	<u>12</u>	<u>8</u>	<u>0</u>	<u>0</u>	Y	C	L	H	Z	Z		25	3	12	8	0	0	- F	X	I	P	U	F	⇒	- 6	24	9	16	21	6	<u>S</u>	<u>E</u>	<u>C</u>	<u>R</u>	<u>E</u>	<u>T</u>	⇐	<u>19</u>	<u>5</u>	<u>3</u>	<u>18</u>	<u>5</u>	<u>20</u>
A	B	C	...	...	...	...	...	X	Y	Z																																																																																																						
↓	↓	↓						↓	↓	↓																																																																																																						
1	2	3						24	25	0																																																																																																						
S	E	C	R	E	T		19	5	3	18	5	20																																																																																																				
+ F	X	I	P	U	F	⇒	+ 6	24	9	16	21	6																																																																																																				
<u>Y</u>	<u>C</u>	<u>L</u>	<u>H</u>	<u>Z</u>	<u>Z</u>	⇐	<u>25</u>	<u>3</u>	<u>12</u>	<u>8</u>	<u>0</u>	<u>0</u>																																																																																																				
Y	C	L	H	Z	Z		25	3	12	8	0	0																																																																																																				
- F	X	I	P	U	F	⇒	- 6	24	9	16	21	6																																																																																																				
<u>S</u>	<u>E</u>	<u>C</u>	<u>R</u>	<u>E</u>	<u>T</u>	⇐	<u>19</u>	<u>5</u>	<u>3</u>	<u>18</u>	<u>5</u>	<u>20</u>																																																																																																				
<p>20 mins</p>																																																																																																																

<p><b>Codes and Ciphers</b></p>	<p><b>UNIT 12 One-Time Pads Lesson Plan 1</b></p>																			
<p><b>Activity</b> <b>2</b></p>	<p><b>Exercises</b></p> <p>T: Now try Exercise 1 in your text.</p> <p>T: Who has the answers? Come and write them on the board.</p> <p>P<sub>1</sub> (writing on board):</p> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 5px auto;">DSNA PFO JLW KI</div> <p>T: To help with security, we usually put the message into groups of 5 letters. Can someone quickly do that for us now?</p> <p>P<sub>2</sub> (on board):</p> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 5px auto;">DSNAP FOJLW KI</div> <p>T: And for part b) ? Remember to arrange the letters in groups of 5.</p> <p>P<sub>3</sub> (on board):</p> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 5px auto;">AOPLC JSANN PQSFG</div> <p>T: Well done!</p> <p style="text-align: right;"><i>30 mins</i></p>	<p style="text-align: center;"><b>Notes</b></p> <p>Ps work in pairs for about 5 minutes, writing in their Ex.Bs.; T monitors their work, intervening if necessary.</p> <p>Volunteer Ps write their answers on board; other Ps agree/disagree. Ps write correct answers in their Ex.Bs.</p> <p>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).</p>																		
<p><b>3</b></p>	<p><b>Subtractive key</b></p> <p>T: You can also use the subtractive key method; here you <u>subtract</u> the key from the message.</p> <p>T: Who would like to encrypt the message on the OS?</p> <p>P<sub>4</sub> (on OS):</p> <div style="border: 1px solid black; padding: 10px; width: fit-content; margin: 5px auto;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: right;">S E C R E T</td> <td style="padding: 0 10px;">⇒</td> <td style="text-align: left;">19 5 3 18 5 20</td> </tr> <tr> <td style="text-align: right;">- F X I P U F</td> <td style="padding: 0 10px;">+</td> <td style="text-align: left;">6 24 9 16 21 6</td> </tr> <tr> <td style="text-align: right; border-top: 1px solid black;">Y C L H Z Z</td> <td style="padding: 0 10px;">⇐</td> <td style="text-align: left; border-top: 1px solid black;">13 7 20 2 10 14</td> </tr> </table> </div> <p>T: Very good.</p> <p>T: How can you decipher the message? <span style="float: right;"><i>(Add the key)</i></span></p> <p>T: Come and show us.</p> <p>P<sub>5</sub> (on OS):</p> <div style="border: 1px solid black; padding: 10px; width: fit-content; margin: 5px auto;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: right;">M G T B J N</td> <td style="padding: 0 10px;">⇒</td> <td style="text-align: left;">13 7 20 2 10 14</td> </tr> <tr> <td style="text-align: right;">+ F X I P U F</td> <td style="padding: 0 10px;">+</td> <td style="text-align: left;">6 24 9 16 21 6</td> </tr> <tr> <td style="text-align: right; border-top: 1px solid black;">S E C R E T</td> <td style="padding: 0 10px;">⇐</td> <td style="text-align: left; border-top: 1px solid black;">19 5 3 18 5 20</td> </tr> </table> </div> <p>T: Well done!</p> <p style="text-align: right;"><i>35 mins</i></p>	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	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	<p><b>OS 12.3</b> on OHP or similar on OS.</p> <p>Volunteer Ps write answers; other Ps agree/disagree.</p> <p>Ps write correct answers in their Ex.Bs.</p>
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																		
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																		
<p><b>4</b></p> <p><i>(continued)</i></p>	<p><b>Activity</b></p> <p>T: Now we'll look at a third method, called 'minuend'. I'll give you 5 minutes to work through Activity 1.</p> <p>T: Who is going to show us how this method works for encrypting?</p> <p>P (at board):</p> <div style="border: 1px solid black; padding: 10px; width: fit-content; margin: 5px auto;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: right;">F X I P U F</td> <td style="padding: 0 10px;">⇒</td> <td style="text-align: left;">6 24 9 16 21 6</td> </tr> <tr> <td style="text-align: right;">- S E C R E T</td> <td style="padding: 0 10px;">⇒</td> <td style="text-align: left;">- 19 5 3 18 5 20</td> </tr> <tr> <td style="text-align: right; border-top: 1px solid black;">M S F X R L</td> <td style="padding: 0 10px;">⇐</td> <td style="text-align: left; border-top: 1px solid black;">13 19 6 24 16 12</td> </tr> </table> </div>	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	<p>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.</p>									
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																		

<p><b>Codes and Ciphers</b></p>	<p><b>UNIT 12 One-Time Pads Lesson Plan 1</b></p>	
<p><b>Activity</b> <b>4</b> <i>(continued)</i></p>	<p>T: Good. Who has decrypted the message? P (on board):</p> <div style="border: 1px solid black; padding: 10px; width: fit-content; margin: 10px auto;"> <math display="block">  \begin{array}{r}  \text{F X I P U F} \quad \Rightarrow \quad 6 \ 24 \ 9 \ 16 \ 21 \ 6 \\  - \text{M S F X R L} \quad \Rightarrow \quad - \ 13 \ 19 \ 6 \ 24 \ 16 \ 12 \\  \hline  \text{S E C R E T} \quad \Leftarrow \quad 19 \ 5 \ 3 \ 18 \ 5 \ 20  \end{array}  </math> </div> <p>T: What is the main problem with these methods of coding and can it be overcome? <i>(Distribution and security of the key)</i></p> <p style="text-align: right;"><i>45 mins</i></p>	<p style="text-align: center;"><b>Notes</b></p> <p>T can point out that minuend key is popular as the same operation (subtracting from the key) is used for both encrypting and decrypting.</p> <p>Whole class discussion of how the key is distributed and kept safe, etc.</p>
	<p><b>Homework</b> Exercise 3 for reinforcement or Activity 2 for creativity</p>	