UNIT 12 One-Time Pads  Lesson Plan 1

Introduction

T: This is another cipher that is dependent on the receiver having a key to help decipher the message.
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.

\[
\begin{array}{cccccccc}
\text{A} & \text{B} & \text{C} & \ldots & \text{X} & \text{Y} & \text{Z} \\
\downarrow & \downarrow & \downarrow & \ldots & \downarrow & \downarrow & \downarrow \\
1 & 2 & 3 & \ldots & 24 & 25 & 0 \\
\end{array}
\]

T: All the arithmetic we use here is 'modulo 26', i.e. remainder on division by 26. So

\[ 16 + 11 = 27 = 1 \pmod{26} \]
\[ 11 \times 5 = 55 = 3 \pmod{26} \]

T: What about

\[ 17 + 17 = ? \pmod{26} \quad (8) \]
\[ 11 - 16 = ? \pmod{26} \quad (?) \]

T: For negative numbers we follow the same rule, so that

\[ 11 - 16 = -5 \]
\[ = -5 + 26 \pmod{26} \]
\[ = 21 \pmod{26} \]

T: What about

\[ 7 - 14 = ? \pmod{26} \quad (19) \]

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.

T: We add together the message and the one-time pad.

Who would like to complete this sheet?

P (on OS):

\[
\begin{array}{ccccccc}
\text{S} & \text{E} & \text{C} & \text{R} & \text{E} & \text{T} & \Rightarrow 19 & 5 & 3 & 18 & 5 & 20 \\
+ \text{F} & \text{X} & \text{I} & \text{P} & \text{U} & \text{F} & \Rightarrow + 6 & 24 & 9 & 16 & 21 & 6 \\
\text{Y} & \text{C} & \text{L} & \text{H} & \text{Z} & \text{Z} & \Leftarrow 25 & 3 & 12 & 8 & 0 & 0 \\
\end{array}
\]

The coded message is YCLHZZ

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):

\[
\begin{array}{ccccccc}
\text{Y} & \text{C} & \text{L} & \text{H} & \text{Z} & \text{Z} & \Rightarrow 25 & 3 & 12 & 8 & 0 & 0 \\
- \text{F} & \text{X} & \text{I} & \text{P} & \text{U} & \text{F} & \Rightarrow - 6 & 24 & 9 & 16 & 21 & 6 \\
\text{S} & \text{E} & \text{C} & \text{R} & \text{E} & \text{T} & \Leftarrow 19 & 5 & 3 & 18 & 5 & 20 \\
\end{array}
\]

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

---

Notes

T: Teacher  P: Pupil  Ex.B: Exercise Book

Whole class discussion on different types of codes.

T shows OS 12.1 (or writes on board); each P has a copy of OS.

Class might need further help here; T could use 'modulo 4' as an initial example.

T chooses Ps to answer the questions – checks that all understand.

T stresses that the answer must be from 0 to 25 but that you can add any positive factor of 26.

More examples might be needed to enforce this concept.

OS 12.2 is shown to help Ps understand the method.

Ps (chosen by T) write on board in turn, helped by other Ps if they are struggling.

Further discussion might be needed for T to check that all Ps have understood the concept.
# UNIT 12 One-Time Pads  Lesson Plan 1

## Activity 2

**Exercises**

T: Now try Exercise 1 in your text.

T: Who has the answers? Come and write them on the board.

P₁ (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?

P₂ (on board):

```
DSNAP FOJLW KI
```

T: And for part b)? Remember to arrange the letters in groups of 5.

P₃ (on board):

```
AOPLC JSANN PQSFG
```

T: Well done!

---

### Notes

Ps work in pairs for about 5 minutes, writing in their Ex.Bs.; T monitors their work, intervening if necessary.

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).

## Activity 3

**Subtractive key**

T: You can also use the subtractive key method; here you subtract the key from the message.

T: Who would like to encrypt the message on the OS?

P₄ (on OS):

```
\[
\begin{array}{cccccc}
S & E & C & R & E & T \\
+ F & X & I & P & U & F \\
Y & C & L & H & Z & Z \\
\hline
M & G & T & B & J & N
\end{array}
\]
```

```
\[
\begin{array}{cccccc}
19 & 5 & 3 & 18 & 5 & 20 \\
+ 6 & 24 & 9 & 16 & 21 & 6 \\
13 & 7 & 20 & 2 & 10 & 14
\end{array}
\]
```

T: Very good.

T: How can you decipher the message? 

(Add the key)

T: Come and show us.

P₅ (on OS):

```
\[
\begin{array}{cccccc}
M & G & T & B & J & N \\
+ F & X & I & P & U & F \\
S & E & C & R & E & T \\
\hline
13 & 7 & 20 & 2 & 10 & 14 \\
+ 6 & 24 & 9 & 16 & 21 & 6 \\
19 & 5 & 3 & 18 & 5 & 20
\end{array}
\]
```

T: Well done!

---

### Notes

Ps write correct answers in their Ex.Bs.

## Activity 4

**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):

```
\[
\begin{array}{cccccc}
F & X & I & P & U & F \\
- S & E & C & R & E & T \\
M & S & F & X & R & L \\
\hline
6 & 24 & 9 & 16 & 21 & 6 \\
- 19 & 5 & 3 & 18 & 5 & 20 \\
13 & 19 & 6 & 24 & 16 & 12
\end{array}
\]
```

---

### Notes

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.
<table>
<thead>
<tr>
<th>Codes and Ciphers</th>
<th>UNIT 12 One-Time Pads  Lesson Plan 1</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activity 4 (continued)</strong></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

T: Good. Who has decrypted the message?

P (on board):

<table>
<thead>
<tr>
<th>F</th>
<th>X</th>
<th>I</th>
<th>P</th>
<th>U</th>
<th>F</th>
<th>6</th>
<th>24</th>
<th>9</th>
<th>16</th>
<th>21</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>M</td>
<td>S</td>
<td>F</td>
<td>X</td>
<td>R</td>
<td>L</td>
<td>13</td>
<td>19</td>
<td>6</td>
<td>24</td>
<td>16</td>
</tr>
<tr>
<td>S</td>
<td>E</td>
<td>C</td>
<td>R</td>
<td>E</td>
<td>T</td>
<td>19</td>
<td>5</td>
<td>3</td>
<td>18</td>
<td>5</td>
<td>20</td>
</tr>
</tbody>
</table>

T: What is the main problem with these methods of coding and can it be overcome? *(Distribution and security of the key)*

45 mins

<table>
<thead>
<tr>
<th>Homework</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Exercise 3 for reinforcement or Activity 2 for creativity</td>
<td></td>
</tr>
</tbody>
</table>