**UNIT 1 Substitution Ciphers**

### Activity 1

**Introduction**

T: We're going to start by looking at a method for hiding messages used by the Romans. This is called a 'Caesar cipher'. Do you know why? *(Named after the Roman Emperor Julius Caesar)*

T: Here is an example. Our message to code is

```
THIS CODE WAS INVENTED BY JULIUS CAESAR
```

Can you think of a quick and easy way to make this secret? *(Move each letter forwards or backwards by one)*

T: Let's move or shift each letter on by three so that

```
A → D
B → E
C → F
M → P
```

T: What can we do to speed up this process and make it easier? *(Make a list for the complete alphabet)*

**OS 1.1**

T: That's right. Who would like to start this task on the board?

| Plain | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| Cipher| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

T: Write the message in code in your Ex.B. Who would like to write their code on the board?

---

**Practice: Exercise 1**

T: Now try Exercise 1 on the sheet.

T: Who has the solution? Please write it on the board.

P (on board):

```
GONE TO WATCH HARLEQUINS. BACK AT SEVEN.
```

---

**Extending the idea**

T: How can we design a different Caesar cipher? *(Shift by different amounts)*

T: How many ways are there of doing this? *(26 ways)*

T: We can see all 26 ways in this grid called a Vigenere square.

This message is coded using one of the shifted alphabets in the Vigenere square. You have 5 minutes, working in pairs, to decode the message.

---

© CIMT, University of Exeter
UNIT 1  Substitution Ciphers  Lesson Plan 1

Caesar Ciphers

Activity 3 (continued)

BPQA PIA JMMV APQNML JG MQOPB
T: Who has found the shift?  (Shift forwards by 8)
T: What is the message?  (THIS HAS BEEN SHIFTED BY EIGHT)
T: How did you work it out?
T: Did anyone use a different method?

25 mins

4 Generalising
T: Why is going through each of the 26 possibilities an inefficient method of coding and decoding?  (Takes too long)
T: Can you think of other ways of tackling this problem?  (?)
T: One method is to consider the letter frequency.  What letter do you think occurs most often?

T: In fact, the first four most frequently used letters, in order, are E T A O
T: Now try Exercise 4 to see if you can decode

VXKT BT RWTTHT EATPH

35 mins

5 Letter frequency
T: Let's try taking a short paragraph of text and finding the letter frequency.  What do we need to help us?  (Tally chart)
T: Draw up a tally chart and write down the number of times each letter occurs in a passage of text of at least 100 letters.

T: What are the four most frequently-occurring letters in your text?  Are they E T A O ?
T: Why do some of you have different results?  (Too small a sample of text)
T: We can get a better idea by adding all your letter frequencies together.  In turn, write your frequencies on this list.

45 mins

Homework
T: Take a passage of text of at least 300 words from any book and work out the letter frequency.  Write the letter frequency in rank order, e.g.

E T A O . . .
**UNIT 1 Substitution Ciphers**

### Activity 1A

**Martian alphabet**

T: The Martian alphabet has only 3 letters:

\[ \Box \bigstar \triangle \]

How many different substitution ciphers can you find for the Martian alphabet? I'll give you 5 minutes to work out the answer.

T: Who thinks that they have the correct answer? (6)

How did you work it out?

T: The Venusian alphabet is similar but has one extra letter, namely \( \heartsuit \).

How many different substitution ciphers can you find for the Venusian alphabet? Don't write them all down - use the answer for the Martian alphabet to help you.

T: Write your answer on your slate/mini-whiteboard: show it now! (24)

T: Why 24? (4 \times 6)

### Activity 1B

T: Now we can deduce the answer for an alphabet with 26 letters.

What is it – as an expression? (26 \times 25 \times \ldots \times 2 \times 1)

T (to P): Write the expression on the board.

T: In fact, its value is 403 291 461 126 605 635 584 000 000 which is a little over 400 million million million million.

### Extension

T: What about an alphabet with \( n \) letters - how many different substitution ciphers will there be? (\( n \times (n - 1) \times \ldots \times 2 \times 1 \))

T: Well done; for convenience, we write this as \( n! = n \times (n - 1) \times (n - 2) \ldots 2 \times 1 \)

\( n! \) is pronounced 'n factorial'.

T: What is the answer using the ‘factorial’ symbol for the Venusian alphabet? (4!)

And for the English alphabet? (26!)

### Activity 2

**Substitution ciphers**

T: What does this message say

ZHCVHYP NYDCTG SJL GCMO

T: Has anyone decoded it?

T: How can we tackle this problem? (With frequency)

T: Good idea. Before we do that, let's first review your homework.
<table>
<thead>
<tr>
<th>Codes and Ciphers</th>
<th>UNIT 1 Substitution Ciphers</th>
<th>Lesson Plan 2 Substitution Ciphers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activity 2</strong></td>
<td>T: Who agrees with the order E T A O for the first four letters? T: What are the next four letters? (Possibly N R I S) T: In fact, overall, in most extended passages of English text, the letter frequency is E T A O N R I S H D L F C U M G P Y W B V K X J Q Z Use this to help decode the message above. T: What is the message? T: Well done! (JANUARY BRINGS THE SNOW)</td>
<td>Notes Interactive discussion on rank order of letter frequency; let Ps display their first 10 letters in descending order of frequency, on the board. OS 1.4 T gives Ps a few more minutes; monitors work, giving helpful hints, etc. Agreement, self-correction. Praising. T encourages Ps to discuss their approach.</td>
</tr>
<tr>
<td><strong>3</strong> Challenge</td>
<td>T: Working in pairs, look at the code on OS 1.5. Use all the facts you have learnt to help you to decode the message and to find the complete substitute alphabet. T: What progress have you made? What letters are you sure about? T: Your task is to decode the passage. You can though use some hints if you think that you need them. You need to complete the task for homework.</td>
<td>At this stage Ps are just given OS 1.5 and the letter frequency table. T monitors progress but does not help. T intervenes after 10 minutes. Interactive discussion, but T still does not give help. T can give Hints 1-3 and Hints 4-6 in separate sealed envelopes (they are listed separately on OS 1.6 and OS 1.7).</td>
</tr>
<tr>
<td><strong>Homework</strong></td>
<td>Complete the task of decoding the passage. Can you complete the substitution cipher? If not, why not? <strong>Extension</strong> Use the internet to find the letter frequencies in other alphabets, e.g. Welsh.</td>
<td></td>
</tr>
</tbody>
</table>

© CIMT, University of Exeter