# Codes and Ciphers — UNIT 19 — *Lorenz Cipher Machine* — Lesson Plan 1

| Activity | | Notes |
|---|---|---|
| | | T: Teacher P: Pupil Ex.B: Exercise Book |
| 1 | **Introduction**<br>T: In this first lesson we'll look at the principles of the Lorenz cipher; in the next lesson we'll learn how the Lorenz cipher machine was used to break the code. | Interactive introduction; T will find out how much the Ps know about code-breaking in the Second World War. |
| | T: We start with the enciphering of letters. Step 1 is to convert letters to binary numbers. | Ps are each given a copy of **OS 19.1**, or it is shown on OHP. |
| | T: How many codes are used for the letters of the alphabet? *(26)*<br>T: Using 5 bits for the digits, how many codes are available? *(32)*<br>T: Why do you say '32' ? *(Because* $2\times2\times2\times2\times2=2^5$*)*<br>T: So how many are left to assign? *(*$32-26=6$*)* | |
| | T: The sheet shows how these codes are used; only '9' is used in messages and it represents a space between words.<br>0 + 0 = 0    0 + 1 = 1<br>1 + 0 = 1    1 + 1 = 0 | T writes on board, and makes sure all Ps are familiar with this (could refer back to **Unit 18** where this type of addition is also used). |
| | T: We add a 'key' to any message in order to make it difficult to break, so we need to define the type of key (or additive) used.<br>T: Let's look at an example. We want to send the letter J using the key letter B, so we actually send J + B. Who can do this?<br>P (on board):<br>J ⇒ 1 1 0 1 0<br>+ B ⇒ 1 0 0 1 1<br>0 1 0 0 1<br>T: Well done. Which letter is this? *(L)*<br>T: So the letter L is sent. Now its time for you to do some examples. | |
| | Encipher A, B, C, D and E using the key letter B. | T gives Ps a few minutes for this; monitors their progress and intervenes if necessary, They should each have a copy of **OS 19.1** to refer to. |
| | T: Who is going to show their answer?<br>5 Ps (on board):<br>A ⇒ 1 1 0 0 0 + B ⇒ 1 0 0 1 1 = 0 1 0 1 1<br>B ⇒ 1 0 0 1 1 + B ⇒ 1 0 0 1 1 = 0 0 0 0 0<br>C ⇒ 0 1 1 1 0 + B ⇒ 1 0 0 1 1 = 1 1 1 0 1<br>D ⇒ 1 0 0 1 0 + B ⇒ 1 0 0 1 1 = 0 0 0 0 1<br>E ⇒ 1 0 0 0 0 + B ⇒ 1 0 0 1 1 = 0 0 0 1 1 | Volunteer Ps work simultaneously at board. Other Ps watch and then T and whole class review the answers, correcting if necessary.<br><br>T should ensure that all Ps understand this form of addition of these binary codes. |
| *(continued)* | | |

| ***Codes and Ciphers*** | **UNIT 19** *Lorenz Cipher Machine* Lesson Plan 1 | |
|---|---|---|
| ***Activity*** | | ***Notes*** |
| **1** *(continued)* | T: What do you notice about B + B *(It is '/')*<br>T: What about A + A or C + C, etc.? *(Also '/')*<br>T: So the '/' symbol is a really important one and was a crucial factor in the original breaking of the code.<br>*10 mins* | Interactive discussion about importance of the '/' symbol. |
| **2** | **Enciphering**<br>T: How can this code be made more secure? *(By using a sequence of key letters which is kept secret)*<br>T: Yes, that's right. We encipher HELP using the key sequence ABCD. Who will show us?<br>P (on board):<br>H E L P ⇒ 00101 \| 10000 \| 01001 \| 01101<br>A B C D + 11000 \| 10011 \| 01110 \| 10010<br>Q O M 8 ⇐ 11101 \| 00011 \| 00111 \| 11111<br>T: Well done. How can the message be made more secure? *(By using a key sequence which is not obvious)*<br>T: Yes. Now try this one. You have 5 minutes to come up with the answer.<br>Encipher LONDON using the key sequence HBVQZM.<br>*20 mins* | Whole class interactive discussion.<br>**OS 19.3** will speed up the process here.<br>T must make sure that the class are understanding this and paying attention – they can take it in turns to do the addition and to identify the letters.<br>Further whole class interactive discussion about ways of making the code more difficult to break.<br>Review answers – volunteer (or chosen by T) Ps can work at board and the class then agree/ disagree with their answers until correct solutions are given. |
| **3**<br>*(continued)* | **Decipher**<br>T: How can we decipher messages we have been sent? *(We will need to know the key sequence)*<br>T: If we have the key sequence, what do we do? *(Reverse the operations for enciphering)*<br>T: Yes, but the reverse if doing the same thing again! Go back to our message QOM8. What do you write?<br>P (at board):<br>H E L P ⇒ 11101 \| 00011 \| 00111 \| 11111<br>A B C D + 11000 \| 10011 \| 01110 \| 10010<br>Q O M 8 ⇐ 00101 \| 10000 \| 01001 \| 01101<br>T: Good. Now I'll give you a few minutes to retrieve LONDON from your last message. | Interactive discussion about the procedures.<br>**OS 19.3** will help the process here.<br>T gives Ps a few minutes; monitors their progress, intervening if there are problems.<br>Answers are checked interactively. |

| ***Codes and Ciphers*** | **UNIT 19** *Lorenz Cipher Machine* Lesson Plan 1 | |
|---|---|---|
| ***Activity*** | | ***Notes*** |
| **3** *(continued)* | T: What takes time in this? *(The addition)*<br>T: The Bletchley Park experts soon memorised each additive; we can make it easier by using a table.<br>*30 mins* | Each pair of Ps has a copy of **OS 19.2** and time is given for them to familiarise themselves with how it is used. |
| **4** | **Simplified Lorenz cipher machine**<br>T: Here is a very simplified Lorenz cipher machine; do you see what it does? *(Uses the code wheels; they change after each turn)*<br>T: Let's see what happens if we send the message THE. First the letter T. With the starting positions shown what happens to it? *(T + A + B)*<br>T: Use your table to work this out. *(R)*<br>T: Each wheel now turns one position. What are they now on? *(B and A)*<br>T: So what is the output for 'H' ? *(H + B + A)*<br>T: And that is ...? *(C)*<br>T: And for 'E' ? *(E + C + A = N)*<br>T: Well done. So the message would be sent as RCN.<br>T: Now you can encipher a message.<br>With starting positions K = 5 and S = 2 encipher<br>SECRET MESSAGE<br>What must you remember to do? *(Put 9 for the space; remember that the wheels move on one position each time)*<br>T: And the message is ....? *(UYFX9 4LFVT 8BQZ)*<br>*45 mins* | Interactive discussion. The real Lorenz machine had twelve wheels and operated in a much more complex way than the simplified version. **OS 19.4** can be shown or each pair of Ps given a copy.<br><br>Ps will need at least 5 minutes for this. T should monitor progress and intervene if necessary.<br><br>T and Ps review the answers together with T making sure that all Ps understand the way the cipher works. |
| | **Homework**<br>Decipher the coded message<br>UYFX9 4LFVT 8BQZ | |
| | | |

# Codes and Ciphers — UNIT 19 *Lorenz Cipher Machine* — Lesson Plan 2 — *Breaking the Cipher*

| *Activity* | | *Notes* |
|---|---|---|

**1**

**Breaking the cipher**

T: The Wartime success at Bletchley Park in breaking this cipher depended upon the fact that most of the German plaintext messages contained many pairs of repeated characters. (There were certain technical reasons why the Germans adopted this practice.)

T: We'll illustrate the technique with the following short message in which the words are separated by double spaces represented by pairs of 9s.

99HERE99IS99A99TEST99MESSAGE99FOR99YOU99TO99TRY99OUT99

T: What is the first coded character? *(9 + G + B = U)*

T: Now you code the next 7 characters. *(9HERE99)*

T: Well done. In fact, the complete coded message is

UDZMR+JMSDC+TXUVQMYEDE8LWOKUD3TMK+G4UDC3NXWKOBYEFURWH

T: The codebreakers at Bletchley Park devised this process. We will not show here why it works (you can read an account if you are interested), but just show that it does work.

T: We'll follow through the process for the first 8 letters of the message.

**1.**

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Z** | = | U | D | Z | D | M | R | + | J |
| $\Delta$**Z** | = | C | O | O | Y | P | Z | T | |

**2.** Here K = 1, so we first find the **K** sequence.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **K** | = | A | B | C | D | E | F | G | H |
| $\Delta$**K** | = | G | Q | U | 3 | N | Q | C | |

**3.**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $\Delta$**Z** | = | C | O | O | Y | P | Z | T |
| $\Delta$**K** | = | G | Q | U | 3 | N | Q | C |
| $\Delta$**Z** + $\Delta$**K** | = | H | K | 8 | X | G | I | V |

**4.** There are no '/'s in this sequence for $\Delta \mathbf{Z} + \Delta \mathbf{K}$.

T: So as there are no '/'s, it is unlikely that K = 1 was the starting position of the K wheel.

T: Now you work through the process using K = 7 and see what happens.

T: How many '/'s did you get? *(2)*

T: Using the complete message, you actually get 7 '/'s.

*25 mins*

*Notes:*

This needs careful handling; Ps need to work through the process but T should not allow it to become too long and tedious. The printout will help with this. Ps with IT skills could perhaps write a program to complete the process.

The class need a few minutes for this; some Ps could work at the board, each tackling a letter, in turn.

T reviews answers with Ps, praising when deserved.

Each P is given a copy of **OS 19.5** and it is shown on OHP.

It is probably best if this is done interactively; Ps either give answers aloud or write them on the board.

T will need to monitor work closely to check that Ps have understood what is required.

**2**

**K wheel positions**

T: By hand, this process is tedious, so here is the printout for each position of the K wheel.

T: Quickly check the number of '/'s in each line of the printout. What do you get? *(3, 1, 1, 2, 1, 0, 7, 1, 1, 2, 1, 6, 2, 2)*

*(continued)*

*Notes:*

Each P has a copy of **OS 19.6**.

T chooses Ps to give answers and the rest of the class agree/ disagree.

| **Codes and Ciphers** | **UNIT 19** *Lorenz Cipher Machine* Lesson Plan 2 | |
|---|---|---|
| ***Activity*** | | ***Notes*** |
| **2** *(continued)* | T: So what was the position of the K wheel? *(7 or 12)*<br>T: In practice, both will need to be checked although we do know in this case that it is 7.<br>*30 mins* | |
| **3** | **S wheel position**<br>T: Taking $K = 7$, we now need to find the position of the S wheel. How can we do this? *(Try each value in turn)*<br>T: OK – starting with $S = 1$ and using just the first 8 letters, what do we get?<br>P (at board): | Interactive discussion; Ps should be able to suggest the method.<br>One P at board; other Ps can help with the calculations, etc. and check what is being written on board. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | U | D | Z | D | M | R | + | J | |
| + | G | H | I | J | K | L | M | N | (K wheel) |
| + | A | A | B | B | A | A | B | B | (S wheel) |
| | V | V | C | + | T | + | V | V | |

| | | |
|---|---|---|
| | T: Does this message make sense? *(No!)*<br>T: Your turn now ....try $S = 2$ and then $S = 3$.<br>T: So we can confirm that $K = 7$ and $S = 3$ are the correct starting positions. What complicates the real problem? *(The starting position of all twelve wheels had to be determined and the number of possible starting positions of the wheels were greater. (They were all within the range 23 to 61.))*<br>T: Yes – this provided the motivation for the development, at Bletchley Park, of 'Colossus', the world's first programable electronic computer.<br>*45 mins* | T will need to give Ps sufficient time to complete this calculation and to confirm that $S = 3$ gives the start of a meaningful message. |
| | **Homework**<br>Go through the same process again with a new short message and confirm that this method of deciphering works. | |