

UNIT 19 *Lorenz Cipher Machine* Teacher Resource Material

Key Stage: 4 / A-level

Target: Gifted and talented students

This is a simplified model for the Lorenz cipher machine – but it is still quite complex. Although messages can be enciphered by following the instructions, deciphering is much more complicated. The method illustrated here simulates what actually happened at Bletchley Park in the Second World War, when the breaking of the Lorenz Code was a very significant breakthrough for the Allies.

We are particularly grateful to Frank Carter (of Bletchley Park) for providing a first version of this resource.

Solutions and Notes

- Exercise 1* $A + B \Rightarrow 11000 + 10011 = 01011 \Rightarrow G$
 $B + B \Rightarrow /$
 $C + B \Rightarrow 01110 + 10011 = 11101 \Rightarrow Q$
 $D + B \Rightarrow 10010 + 10011 = 00001 \Rightarrow T$
 $E + B \Rightarrow 10000 + 10011 = 00011 \Rightarrow O$

- Exercise 2* LONDON \Rightarrow 01001 | 00011 | 00110 | 10010 | 00011 | 00110
 HBVQZM + 00101 | 10011 | 01111 | 11101 | 10001 | 00111
 IELVDT \Leftarrow 01100 | 10000 | 01001 | 01111 | 10010 | 00001

- Exercise 3* IELVDT \Rightarrow 01100 | 10000 | 01001 | 01111 | 10010 | 00001
 HBVQZM + 00101 | 10011 | 01111 | 11101 | 10001 | 00111
 LONDON \Leftarrow 01001 | 00011 | 00110 | 10010 | 00011 | 00110

- Activity 1* $2^5 = 32$ codes.
 All codes are needed as adding two codes might give a code that is not used.

- Exercise 4* $S + E + A = G + A = U$
 $E + F + B = N + B = Y$
 $C + G + B = H + B = F$
 $R + H + A = V + A = X$
 $E + I + A = U + A = 9$
 $T + J + B = + + B = 4$
 $9 + K + B = J + B = L$
 $M + L + A = C + A = F$
 $E + M + A = X + A = V$
 $S + N + B = D + B = T$
 $S + A + B = I + B = 8$
 $A + B + A = G + A = B$
 $G + C + A = H + A = Q$
 $E + D + B = 3 + B = Z$

Enciphered message UYFX9 4LFVT 8BQZ

UNIT 19 *Lorenz Cipher Machine* Teacher Resource Material (continued)

Exercise 5 $U + E + A = I + A = S$
 $Y + F + B = O + B = E$, etc.

Exercise 6 $9 + G + B = V + B = U$
 $9 + H + B = T + B = D$
 $H + I + A = L + A = Z$
 $E + J + A = R + A = D$
 $R + K + B = S + B = M$
 $E + L + B = W + B = R$
 $9 + M + A = 0 + A = +$
 $9 + N + A = 3 + A = J$

i.e. UDZDMR+J

- Exercise 7* 1. $\Delta Z = \text{COOYPZT}$
 2. For starting position 7,

$$\begin{array}{cccccccc} \mathbf{K} & = & \mathbf{G} & \mathbf{H} & \mathbf{I} & \mathbf{J} & \mathbf{K} & \mathbf{L} & \mathbf{M} & \mathbf{N} \\ \Delta \mathbf{K} & = & \underbrace{\mathbf{C}} & \underbrace{\mathbf{L}} & \underbrace{\mathbf{F}} & \underbrace{\mathbf{9}} & \underbrace{\mathbf{X}} & \underbrace{\mathbf{C}} & \underbrace{\mathbf{T}} & \end{array}$$

$$\begin{array}{cccccccc} 3. & \Delta \mathbf{Z} & = & \mathbf{C} & \mathbf{O} & \mathbf{O} & \mathbf{Y} & \mathbf{P} & \mathbf{Z} & \mathbf{T} \\ & \Delta \mathbf{K} & = & \mathbf{C} & \mathbf{L} & \mathbf{F} & \mathbf{9} & \mathbf{X} & \mathbf{C} & \mathbf{T} \\ \hline & \Delta \mathbf{Z} + \Delta \mathbf{K} & = & / & \mathbf{R} & \mathbf{Y} & \mathbf{Z} & \mathbf{J} & \mathbf{8} & / \end{array}$$

4. There are two '/'s in this sequence.

Activity 2 No. of '/'s: $K = 1, 3; K = 2, 1; K = 3, 1; K = 4, 2; K = 5, 1; K = 6, 0; K = 7, 7$
 $K = 8, 1; K = 9, 1; K = 10, 2; K = 11, 1; K = 12, 6; K = 13, 2; K = 14, 2$

The greatest number of '/'s occur when $K = 7$.

Activity 3

$$\begin{array}{cccccccc} & \mathbf{U} & \mathbf{D} & \mathbf{Z} & \mathbf{D} & \mathbf{M} & \mathbf{R} & + & \mathbf{J} \\ + & \mathbf{G} & \mathbf{H} & \mathbf{I} & \mathbf{J} & \mathbf{K} & \mathbf{L} & \mathbf{M} & \mathbf{N} \\ + & \mathbf{B} & \mathbf{B} & \mathbf{A} & \mathbf{A} & \mathbf{B} & \mathbf{B} & \mathbf{A} & \mathbf{A} \\ \hline & \mathbf{9} & \mathbf{9} & \mathbf{H} & \mathbf{E} & \mathbf{R} & \mathbf{E} & \mathbf{9} & \mathbf{9} \end{array}$$

Hence $S = 3$ will recover the message.