UNIT 20 *Enigma Cipher* Teacher Resource Material

Key Stage: *4*

Target: *Gifted and talented students (of any age!)*

Some of the ideas and methods used in earlier units are brought together here, where the focus is essentially on showing the numbers of possible configurations for the Enigma Cipher Machine, and hence the enormity of breaking this code. We deal, in a very simplified way, with some of the methods used.

Websites with information relevant to this topic include

- http://www.bletchleypark.org.uk
- http://www.codesandciphers.co.uk
- http://homepages.tesco.net/~andycarlson/enigma/about_enigma.html
- http://www.nsa.gov/museum/museu00007.cfm
- http://www.iwm.org.uk/upload/package/10/enigma/index.htm
- http://www.simonsingh.net (see this site for details of CD-ROM on codes).

We are particularly grateful for permission to use material produced earlier by Frank Carter (Bletchley Park) and Claire Ellis.

Solutions and Notes

Exercise 1 $5 \times 4 \times 3 = 60$ ways, as there are 5 choices for the first rotor, 4 for the next, etc.

Exercise 2 $26 \times 26 \times 26 = 17576$ different ways

Activity 1 a) $5 + 4 + 3 + 2 + 1 = 15$ ways b) 45 ways c) 15 ways

2 is the optimum number to use as it gives the maximum number of connections.

Activity 2

n *(number of pairs)*	*Number of possibilities*
1	325
2	44 850
3	3 453 450
4	164 038 875
5	5 019 589 575
6	100 391 791 500
7	1 305 093 289 500
8	10 767 019 638 375
9	58 835 098 191 875
10	150 738 274 937 250
11	205 552 193 096 250
12	102 776 096 548 125
13	7 905 853 580 625

(These numbers might seem improbable, but look at the number of ways you can put 2 pieces of wire into 6 plugboard sockets: there are 45 ways, three times as many as you get with 3 wires.)

UNIT 20 *Enigma Cipher* Teacher Resource Material (continued)

Exercise 4 ANENIGMACIPHER

Exercise 5 Q $\rightarrow$ A on lines 3 and 7. We will try each one in turn.

Line 3: The message becomes ??QSABHYURFTAVP which doesn't seem to make any sense.

Line 7: YOUHAVEDONEWELL

So the message sent is 'YOU HAVE DONE WELL'

Exercise 6 Q $\rightarrow$ E on lines 16 and 18, but Z $\rightarrow$ N on lines 9 and 17. So it is clear that we use lines 16 and 17 for the last two letters. Hence we start the message on line 4, to give

THISISANEASYONE

so the message is 'THIS IS AN EASY ONE'.