Codes and Ciphers — UNIT 20 *Enigma Cipher* Lesson Plan 1

Activity		Notes T: Teacher P: Pupil Ex.B: Exercise Book
1	**Introduction** T: The Enigma cipher machine, which was invented in 1915, was used by the German armed forces to encrypt messages during the Second World War. Inside the machine were slots for 3 rotors; each rotor had letters A to Z with different internal wiring. The rotors could be taken out and changed and there were 5 different rotors for the 3 slots. T: How many different ways are there of positioning 5 rotors in 3 slots? *(*$5 \times 4 \times 3 = 60$ *ways)* T: The rotor starting point could be any one of 26 positions (A to Z). How many different ways can you set the starting positions of the 3 rotors? *(*$26 \times 26 \times 26 = 17\,576$ *ways)* T: Using the calculations we have just made, how many possible ways are there of setting up the rotors? *(*$60 \times 17\,576$*)* T: And that is ...? *(*1 054 560*)* T: Yes – over a million different ways. *10 mins*	Discussion for T to find out what Ps might already know about Enigma. Use material from the Pupil Text to give background information. The key aim here is to determine the total number of possible settings so that Ps can appreciate the enormity of the problems encountered in cracking this code. There should be interactive discussion here; if Ps have problems with this, T should use some simple problems for clarification.
2 *(continued)*	**Plugboard** T: On the front of the machine was another variable section called the *plugboard.* This was used to further scramble the messages, and increase the possible number of ways the machine could be set up. The Enigma machine had several cables with a plug at each end that could be used to plug pairs of letters together on the plugboard. If A were plugged to B then upon typing the letter A, the electric current would follow the path through the machine that was normally associated with the letter B, and vice versa. T: If you had just one cable, in how many ways could the plugboard be set up? I'll let you have a few minutes to work this out. T: Who's ready to show us a solution? P_1 (on board): $25 + 24 + ... + 2 + 1$ A with one of the 25 other letters — B with one of the 24 other letters T: Good. How can we solve this quickly? P_2: Use the formula $\boxed{S_n = \frac{n(n+1)}{2}}$ T: Well done. With $S_{25} = 25 + 24 + ... + 2 + 1$ $S_{25} = 1 + 2 + ... + 25 + 26$ $2S_{25} = 26 \times 26 + ... + 26 + 26$ $= 25 \times 26$	It would be helpful to have access to Simon Singh's CD (see Teacher Resource Material) at this stage. This can be used to illustrate how both the rotors and the plugboard work. **OS 20.1** can be shown to illustrate the plugboard. T monitors Ps' work, walking among them to see what they are doing and giving advice where necessary. If little progress is being made, T should intervene and begin checking the solution with the whole class, making sure that Ps understand the reasoning. Volunteer Ps give solutions, P_1 writing on board; P_2 giving solution verbally with T writing on board. T writes on board.

Codes and Ciphers	**UNIT 20** *Enigma Cipher* Lesson Plan 1	
Activity		***Notes***
2 *(continued)*	T: So $S_{25} = ?$ *(* $25 \times 13 = 325$ *)* T: That's the problem solved for just one cable. Now we'll look at more than one cable. Let's start with a plugboard with just 6 letters and 1, 2 or 3 cables. T: How many connections can be made using 1, 2 or 3 cables? T: Who's going to show us their answers and methods? *(*15 with 1 cable; 45 with 2 cables; 15 with 3 cables*)* T: What number of cables gives the largest number of connections? *(2)* T: Right. It's easier if we use a formula when we start looking for the number of connections for 26 letters! T: The formula is $\boxed{\dfrac{n!}{(n-2m)!\,m!\,2^m}}$ T: In fact, the Germans used 10 cables, so $n = 26$ and $m = 10$. Use the formula to work out the number of possible ways of connecting the 26 letters on the plugboard using 10 cables. T: Answer? *(About* 1.5×10^{14}*)* T: Well done. *35 mins*	Volunteer (or chosen by T) P gives the answer. Ps have up to 10 minutes for this activity but T should intervene if little progress is being made. Discussion, with volunteer Ps giving answers and others making suggestions if they disagree. Ps show their methods. T shows the formula on **OS 20.2** and uses it to illustrate the method with $n = 6$, $m = 2$ as an example. T gives Ps time to calculate this; perhaps one P could work at the w/board. Discussion and solution.
3	**Total number of settings** T: Now we'll look at the total number of ways of setting up the electrical circuits on the three rotor Enigma machine. How do we do this? P: The total number is the number of set-up positions for the rotors $\times$ the number of ways of setting up the plugboard. T: Let's use the actual numbers: P: $(60 \times 17\,576) \times (1.5 \times 10^{14})$ T: And this is approximately ...? *(* 1.58×10^{20} *)* T: We can see that cracking the code was not easy! *45 mins*	Interactive discussion at this stage; T introduces deciphering, with the use of a crib if time allows.
	Homework Work through the section in the Pupil Text on 'Deciphering Enigma'.	Copies of Pupil Text pages 5, 6 and 7 distributed to Ps.