Enigma

Jack Copeland

1. Turing Joins the Government Code and Cypher School

Turing's personal battle with the Enigma machine began some months before the outbreak of the Second World War.[1] At this time there was no more than a handful of people in Britain tackling the problem of Enigma. Turing worked largely in isolation, paying occasional visits to the London office of the Government Code and Cypher School (GC & CS) for discussions with Dillwyn Knox.[2] In 1937, during the Spanish Civil War, Knox had broken the type of Enigma machine used by the Italian Navy.[3] However, the more complicated form of Enigma used by the German military, containing the *Steckerbrett* or plug-board, was not so easily defeated.

On 4 September 1939, the day following Chamberlain's announcement of war with Germany, Turing took up residence at the new headquarters of the Government Code and Cypher School, Bletchley Park.[4] GC & CS was a tiny organization

[1] Letters from Peter Twinn to Copeland (28 Jan. 2001, 21 Feb. 2001). Twinn himself joined the attack on Enigma in February 1939. Turing was placed on Denniston's 'emergency list' (see below) in March 1939, according to 'Staff and Establishment of G.C.C.S.' (undated), held in the Public Record Office: National Archives (PRO), Kew, Richmond, Surrey (document reference HW 3/82). (I am grateful to Ralph Erskine for drawing my attention to this document.)

[2] Letters from Twinn to Copeland (see n. 1).

[3] M. Batey, 'Breaking Italian Naval Enigma', in R. Erskine and M. Smith (eds.), *Action This Day* (London: Bantam, 2001), 98.

[4] Letter from A. G. Denniston to T. J. Wilson of the Foreign Office (7 Sept. 1939). PRO document reference FO 366/1059.

ill prepared for war. By 1942, however, Bletchley Park had become a veritable factory, and with the help of the codebreaking machines called 'bombes'—designed by Turing, Gordon Welchman, and, on the engineering side, Harold Keen—GC & CS was deciphering about 39,000 Enigma messages each month.[5] By 1945 almost 9,000 people were employed at Bletchley Park.[6] It is estimated that the breaking of Enigma—and in particular the breaking of Home Waters Naval Enigma, in which Turing played the crucial role—may have shortened the war in Europe by some two years.[7]

Figure 1. The Mansion, Bletchley Park.

Source: Bletchley Park Trust.

The Government Code and Cypher School had developed from the old 'Room 40', established by the Admiralty during the First World War for the purpose of reading enemy ciphers.[8] A branch of the Foreign Office, GC & CS was located in

[5] F. H. Hinsley et al., *British Intelligence in the Second World War*, vol. ii (London: Her Majesty's Stationery Office, 1981), 29.

[6] F. H. Hinsley et al., *British Intelligence in the Second World War*, vol. iii, part 1 (London: Her Majesty's Stationery Office, 1984), 461.

[7] This estimate was given by Hinsley, official historian of the British Secret Service, on p. 12 of his and Alan Stripp's edited volume *Codebreakers: The Inside Story of Bletchley Park* (Oxford: Oxford University Press, 1993). If, wrote Hinsley, the achievements of GC & CS 'had not prevented the U-boats from dominating the Atlantic . . . it is not unreasonable to believe that . . . Overlord [the invasion of Normandy, 1944] would have had to be deferred till 1946'.

[8] The older spelling 'cypher' and the newer 'cipher' were both in use at GC & CS during 1939–45. Mahon used 'cypher' in a 1945 document, part of which forms Chapter 5, and Turing used 'cipher' in a 1940 document, parts of which appear in Chapters 5 and 6.

Whitehall until the summer of 1939.[9] By the beginning of 1938 the Director of Naval Intelligence, Admiral Hugh Sinclair, was looking for premises outside London to which GC & CS could move in the event of war. Bletchley Park—a large Victorian mansion with ample grounds situated in the town of Bletchley, a major railway junction linking London, Oxford, and Cambridge—was purchased in the spring of 1938 (out of Sinclair's own pocket, it is said).

In the course of 1937 and 1938 Commander Alastair Denniston, Head of GC & CS and a veteran of Room 40, supervised a clandestine programme of recruitment, centred largely on Oxford and Cambridge. Denniston's aim was to build up what he described as an 'emergency list [of] men of the Professor type'[10].

> At certain universities . . . there were men now in senior positions who had worked in our ranks during 1914–18. These men knew the type required. Thus it fell out that our most successful recruiting occurred from these universities. During 1937 and 1938 we were able to arrange a series of courses to which we invited our recruits to give them even a dim idea of what would be required of them . . . These men joined up in September 1939.[11]

(Frank Adcock and Frank Birch, the two veterans of Room 40 who were most active in recruitment as the new war approached, were both from the same college as Turing, King's.[12]) In the days following the outbreak of war in September 1939 a group of about thirty people assembled at Bletchley Park, many of them—including Turing—drawn from Denniston's 'emergency list'.[13]

An organizational structure rapidly began to emerge at Bletchley, newly formed sections being known simply as 'Hut 4', 'Hut 6', and so on. The 'huts' were single-storey wooden structures hastily constructed in the grounds of the mansion. Here dons worked among uniformed Naval and Army personnel. Military discipline never took root among the 'men of the Professor type' and parts of Bletchley Park had something of the atmosphere of an Oxbridge college. There were some notable eccentrics among the codebreakers. Dilly Knox, another fellow of King's and veteran of Room 40, liked to work in a hot bath. Once, at his lodgings, Knox

> stayed so long in the bathroom that his fellow-lodgers at last forced the door. They found him standing by the bath, a faint smile on his face, his gaze fixed on abstractions, both taps full on and the plug out. What then was passing in his mind could possibly have solved a problem that was to win a battle.[14]

[9] Probably in August (R. Erskine, 'GC and CS Mobilizes "Men of the Professor Type"', *Cryptologia*, 10 (1986), 50–9 (50)).

[10] Letter from Denniston to Wilson (3 Sept. 1939). PRO document reference FO 366/1059.

[11] A. G. Denniston, 'The Government Code and Cypher School between the Wars', in C. W. Andrew (ed.), *Codebreaking and Signals Intelligence* (London: Cass, 1986), 52.

[12] Andrew, *Codebreaking and Signals Intelligence*, 4.

[13] S. Milner-Barry, 'Hut 6: Early Days', in Hinsley and Stripp (eds.), *Codebreakers*, 90; 'Staff and Establishment of G.C.C.S.'; Erskine, 'GC and CS Mobilizes "Men of the Professor Type"', 50.

[14] E. R. Vincent, Unpublished Memoirs, Corpus Christi College Archives, Cambridge; quoted in C. W. Andrew, *Secret Service: The Making of the British Intelligence Community* (London: Guild, 1985), 94.

It was Knox's Research Section that Turing joined upon his arrival at Bletchley Park.

2. The Enigma Machine

The Enigma machine had something of the appearance of an old-fashioned typewriter. Designed by the Berlin engineer Arthur Scherbius, Enigma was marketed commercially from 1923.[15] In 1926 the German Navy adopted Enigma, followed by the German Army in 1928 and the German Air Force in 1935.[16] At the outbreak of war with Britain, Enigma was the Germans' principal method for protecting their military communications. In 1930, the German military had considerably enhanced the security of the machine by adding the *Steckerbrett* or *plug-board* (see Figure 4).[17] It is this form of Enigma—German military, or *Wehrmacht*, Enigma—that is dealt with here. Successive modifications were made to the operating procedures of the military machine, resulting in substantial variation both over time and from one branch of the armed services to another.

Battery powered and highly portable, the *Wehrmacht* Enigma machine could be used from a general's office in Berlin, an armoured vehicle, a submarine, or a trench. The machine's keyboard had twenty-six keys, each marked with a letter (Figure 4). Instead of an arrangement for typing letters onto paper, the machine had a lampboard consisting of twenty-six bulbs, each of which shone through a stencil on which a letter of the alphabet was marked. The operator of the Enigma machine would be handed a message in plain text. His job was to type the message at the keyboard of the machine. Each time he pressed a key, a letter on the lampboard would light up. The operator's assistant kept a note of which letters lit up on the lampboard. This enciphered form of the message was then sent to its recipient, if by radio then in Morse code. The sending radio operator would preface the message with his radio call-sign, followed by that of the intended receiver. The Germans also sent Enigma messages by land-lines; for these messages, Morse was not used. (Land-lines are not mentioned further in this introduction, since German message traffic sent in this way was not intercepted in Britain.)

Each time the operator pressed a key, one or more wheels turned inside the machine, and each time a wheel moved it altered the wiring between the keyboard and the lampboard. So if, for example, the operator repeatedly depressed the O-key, the connections between the key and the lampboard would change with each key press, resulting in a succession of different letters lighting up, for example Q M P W A J Y R.

[15] F. L. Bauer, *Decrypted Secrets: Methods and Maxims of Cryptology* (Berlin: Springer-Verlag, 2nd edn. 2000), 107.

[16] F. H. Hinsley et al. *British Intelligence in the Second World War*, vol. iii, part 2 (London: Her Majesty's Stationery Office, 1988), 946.

[17] M. Rejewski, 'Remarks on Appendix 1 to British Intelligence in the Second World War by F. H. Hinsley', *Cryptologia*, 6 (1982), 75–83 (76).

Figure 2. A three-wheel Enigma with the plug-board (at the front of the machine) exposed. The lampboard is behind the keyboard. The three wheel-slots are visible behind the lampboard. Beside each wheel-slot is a window through which letters marked on the wheels are visible to the operator.

Source: Science and Society Picture Library, National Museum of Science and Industry.

Figure 3. Enigma machine with the three wheels exposed.
Source: Science and Society Picture Library, National Museum of Science and Industry.

The letter O itself would never appear in this succession of letters, however. Because of the action of the reflector, a letter was never enciphered as itself (see Figure 4). This rule was very useful to the codebreakers at Bletchley Park.

At the receiving end of the radio link, the message would be converted from Morse into ordinary letters. This cipher text was then typed at the keyboard of the recipient's Enigma machine. The letters that lit up on the lampboard would be the very same letters that the sender had keyed in—the plain text with which the process had begun. The design of the Enigma machines was such that if a key was pressed on one machine, say O, and the letter that lit up on the machine's

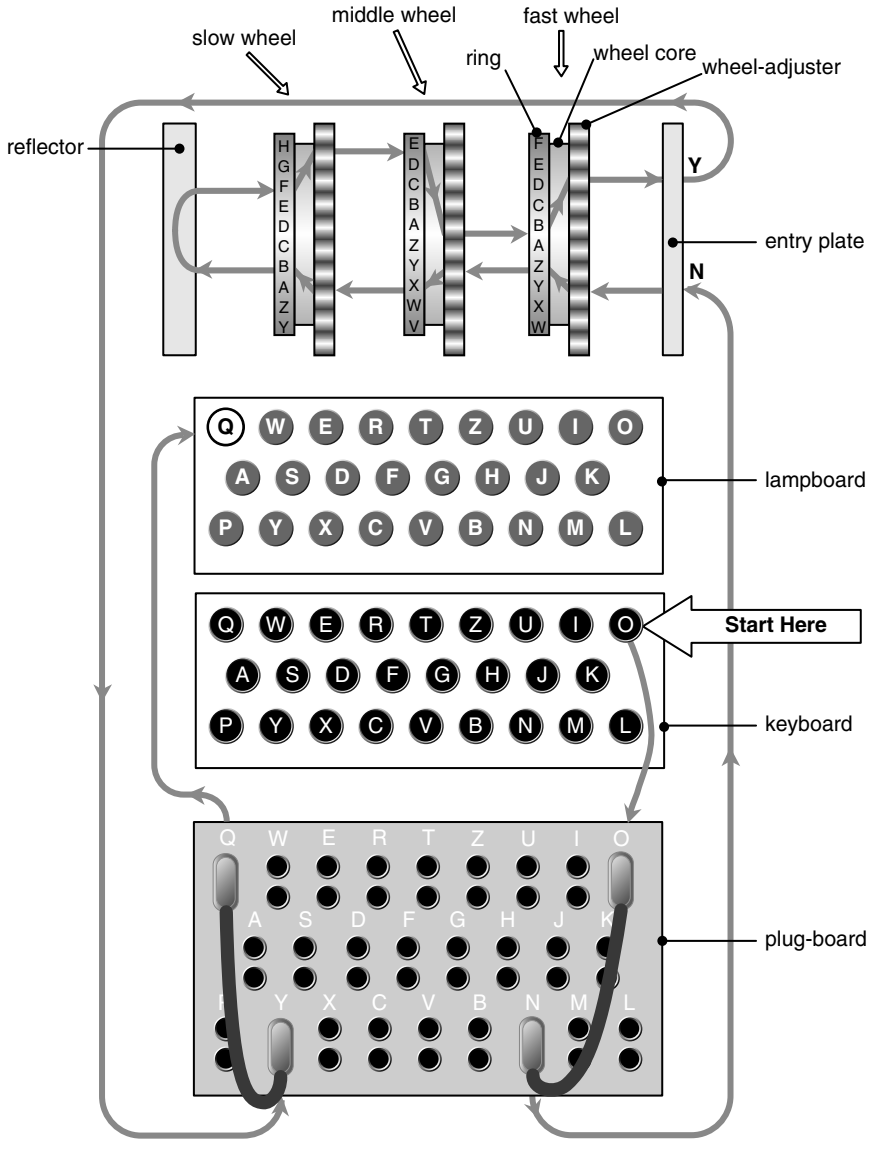

Figure 4. Path of electric current through the Enigma. Pressing a key at the keyboard causes a letter to light up at the lampboard. The core of each wheel contains a maze of 26 insulated wires, with each wire joining one of 26 contacts on the right hand side of the wheel to one of 26 contacts on the left-hand side. The wiring is different in each wheel. Diagram by Dustin A. Barrett.

lampboard was keyed into a second machine, then—provided the two machines had been set up in exactly the same way by their respective operators—the second machine would light up O on its lampboard.

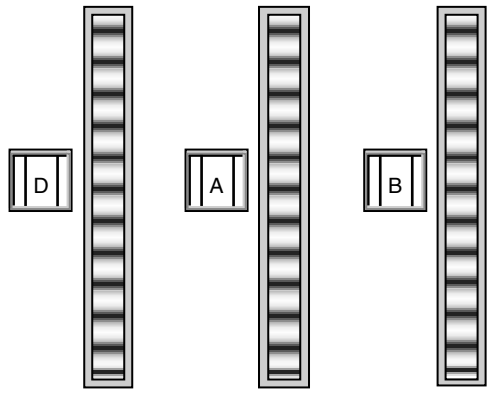

Figure 5. View of the wheels with the case closed. The three wheel-adjusters protrude through slots in the case. The windows allow the operator to see one letter from the ring of each wheel. The 'message setting' is the triple of letters visible at the start of typing a message.

Diagram by Dustin A. Barrett.

In a word, the letter-substitutions were *reversible*: if O produced Q (for example) then, at the same machine-settings, Q produced O. This was the basic principle of the Enigma system, hard-wired into the machine. Figure 4 indicates how this was achieved. If Q were pressed at the keyboard, current would flow along a wire leading to Q at the plug-board, then across the plug-board to Y and through the wheels in the reverse direction to that shown, exiting the wheels at N, crossing the plug-board to O, and lighting O at the lampboard.

The Plug-Board (Steckerbrett) and Wheels

The operator could make various changes to the settings of his machine before he began typing a message at the keyboard. The recipient would set up his own machine in the same way in order to decode the message. How the recipient knew which settings to use is explained in what follows.

The settings of the machine could be changed in the following ways. (See Figure 4.)

1. The operator could make alterations to the plug-board (*Steckerbrett*) on the front of the machine, pulling electrical leads out of sockets and plugging them back into different sockets. This altered some of the connections between the keyboard and the lampboard. (The plug-board was absent from the commercial version of the machine.[18])

[18] The commercial model remained on sale after the German military adopted Enigma. The Germans knew how to break the commercial model and from 1938 several hundred were sold to neutral Switzerland by the German manufacturers. The commercial model was also sold by Germany to Hungary during the war. Commercial model Enigmas sold to Spain were used during the Spanish Civil War. (I am grateful to Frode Weierud for this information (personal communication).)

2. The operator could alter the positions of the rotating wheels inside the machine (sometimes also called 'rotors') by turning them manually. Part of the circumference of each wheel protruded through the case of the machine enabling the operator to click the wheels round with his thumb or finger (Figure 5). In the early years of the war there were three rotatable wheels inside the machine; in 1941, the first Naval machines with a fourth rotatable wheel came into use (see the introduction to Chapter 8).[19] (Another two components of the Enigma are sometimes referred to as wheels or rotors, the *Umkehrwalze* (described by Mahon on p. 269 of Chapter 5) and the *Eintrittwalze*. In the forms of German military Enigma discussed here, both these components were stationary, and they will be referred to as the *reflector* and the *entry plate* respectively (Figure 4).)
3. The operator could open the case of the machine, lift out two or more of the wheels, and replace them in a different order. For example, he might switch the left- and right-hand wheels, leaving the centre wheel untouched. Each wheel was wired differently inside. Since the electrical pathways from the keyboard to the lampboard passed through the wheels, changing the order of the wheels altered the pathways. Alternatively, rather than simply switching the order of the wheels in the machine, the operator might replace one or more of them with different wheels from a box that accompanied the machine. From December 1938 until about the beginning of the war, there were a total of five wheels, numbered I–V, and any three of the five might be inside the machine at any one time. For example, the wheels in use might be I, II, and IV, in the order IV/I/II. From 1940 (or possibly as early as 1939) Enigma machines used by the German Navy were equipped with additional wheels and the operator would select three from a total of eight (numbered I–VIII).

The wheels were somewhat analogous to the wheels of a combination lock, turning through a number of discrete positions. Each wheel had a total of twenty-six possible rotational positions, A–Z. The wheel on the right, the first on the path from keyboard to lampboard, would always turn on one 'click' each time a key was pressed. Hence the term 'fast wheel' (Figure 4). After a certain number of clicks, this wheel would cause the centre wheel to turn one click. Likewise, the centre wheel would at some point cause the wheel on the left—the 'slow wheel'—to move one click. (An extra complication: when this happened, the centre wheel would itself turn forward one click also.[20])

[19] The fourth wheel differed from the other three in that once the operator had set it to one of its twenty-six positions, it remained stationary during the encipherment of the message. (That the fourth wheel came into Naval use in 1941 is documented in R. Erskine, 'Breaking German Naval Enigma on Both Sides of the Atlantic', in Erskine and Smith (eds.), *Action this Day*, 181.

[20] H. Alexander, 'Cryptographic History of Work on the German Naval Enigma' (no date (*c.*1945), PRO document reference HW 25/1), 3; a digital facsimile of Alexander's typescript is available in The Turing Archive for the History of Computing <www.AlanTuring.net/alexander_naval_enigma>.

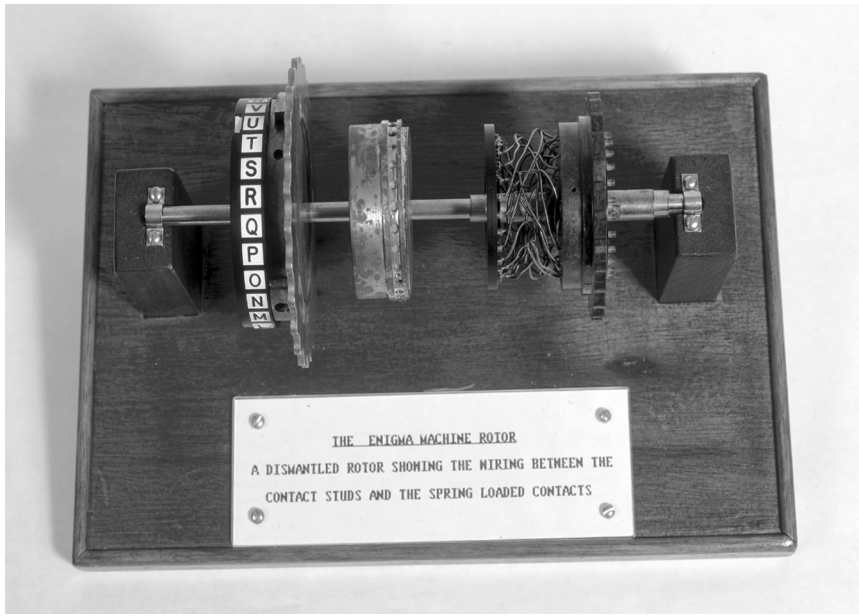

Figure 6. A dismantled wheel.

Source: Science and Society Picture Library, National Museum of Science and Industry.

Precisely when a wheel would cause its neighbour to turn was determined by the position of a notch cut into the ring of the wheel. Since wheels I–V all had their notches in different places, changing or rearranging wheels could affect the 'turnovers' (Bletchley's term for the points at which wheels would cause their neighbours to turn). The Naval wheels VI–VIII were slightly different. These had their notches in the same places as one another, and moreover each had *two* notches (see pp. 268, 285 below). The extra notch meant that in the course of one revolution, the doubly notched wheel would cause its neighbour to move twice.

Which letter lit up on the lampboard depended, therefore, not only on which key was depressed, but also on how the plug-board was connected up, which of the possible wheels were inside the machine, what order these wheels were arranged in, and which of its twenty-six rotational positions each wheel occupied at the time the key was pressed. In fact, by altering these variables, the operator was able to set up a machine with a total of three wheels in excess of a thousand million million different ways. The message remained protected even if the enemy captured an Enigma machine of the type that the sender was using. In order for a recipient to decipher the message, he or she needed to know which of the astronomically many possible settings the sender had used to encipher the text.

Enigma Keys

The sender and the (authorized) recipient were issued with printed tables of settings so that they could set up their machines in the same way. A group of Enigma-users operating with the same tables is called a *network*. A set of tables covered a period of one month and specified how, on any given day, the members of the network should set up their machines. Different networks used different tables.

GC & CS referred to a network of Enigma-users as a 'key'. Each key was given a name—Yellow, Red, Green, Light Blue, Shark, Dolphin, Porpoise, Kestrel, Phoenix, Locust, Snowdrop, etc. At the beginning of the war, the number of known keys was small enough for GC & CS to be able to represent them on a chart by means of coloured pencils, the colour used becoming the name of the key. As the war progressed, the number of keys became much larger.

The term 'network' is perhaps clearer than 'key', especially since at Bletchley, 'key' was used ambiguously for a network of Enigma-users and in the term 'daily key' (whose meaning is explained below). Some writers prefer 'crypto-net' to 'network', since the former term makes it clear that it is an Enigma network and not a radio network that is being described.[21] One and the same radio network could carry the message traffic of several crypto-nets.

Wheel Order, Stecker, and Ringstellung

The wheel order for a particular day for a certain network or key might be III/I/II, for example.

Stecker is short for *Steckerverbindungen*, meaning 'plug connections'. The *Stecker*, or plug-board configuration, for a particular day might be A/C, D/V, F/M, H/W, L/X, R/I. Corresponding to each letter on the plug-board is a pair of sockets, one for a cable leading *to* another letter, and one for a cable leading *from* another letter (Figure 4). The operator would set up the plug-board by connecting together the pair of sockets labelled 'A' and the pair of sockets labelled 'C' by means of a short cable with a double plug at each end. Likewise for the 'D' sockets and the 'V' sockets, and so on. The Germans' use of double plugs meant that if A is steckered to C, then C is steckered to A—a fatal simplification, as we shall see.

Ringstellung means 'ring position'. The ring is like a tyre mounted round the core of each wheel. It is marked with the letters of the alphabet, one for each of the twenty-six rotational positions of the wheel (Figure 4). (Sometimes the numerals '01' to '26' were used instead of letters.) The ring could be moved around the wheel core to a selected position and then fixed in position with a clip. The day's ring position for a given wheel was specified by a single letter, say X. The operator would turn the ring until the letter X was aligned against a fixed

[21] See, for example, G. Welchman, *The Hut Six Story: Breaking the Enigma Codes* (Kidderminster: M. & M. Baldwin, 2nd edn. 1997), 205.

index mark embossed on the wheel and then would fix the ring in this position. The complete *Ringstellung* for the day would consist of a trigram, say XYZ, one letter for each wheel in the machine.

The Daily Key

The daily wheel order, *Stecker*, and *Ringstellung* for the machine were specified in the tables issued to each Enigma network. *Stecker*, wheel order, and *Ringstellung* were elements of the *daily key*, or basic settings for the day for a given network of Enigma users.

The reason for changing the basic settings daily was to minimize the number of messages encoded at the same settings. The Germans knew that security could be compromised if too many messages were encoded at the same basic settings. During the later years of the war, some networks changed the *Stecker*, wheel order, and *Ringstellung* not daily but every eight hours.[22]

The Message Setting

Setting up the sender's and recipient's machines in accordance with the specified *Stecker*, wheel order, and *Ringstellung* did not suffice to place the two machines completely in register. There was also the question of the rotational positions of the three wheels at the start of the message.

Once the ring position was set, the rotational position of a wheel could be described by saying which of the letters on the ring was uppermost when the wheel was in place inside the machine. The machine's case was fitted with three small windows, one above each wheel, so that the operator could see the uppermost letter (Figure 5).

The positions occupied by the wheels at the start of typing a message were specified by a trigram, for example QVZ, meaning that Q is visible in the window over the left-hand wheel, V in the window over the middle wheel, and Z in the window over the right-hand wheel. QVZ was known as the *message setting*.[23]

Notice that knowing the message setting does not reveal the rotational positions of the wheels at the start of the message unless the *Ringstellung* is also known—QVZ may specify any one of the $26 \times 26 \times 26$ possible positions, depending on which ring positions have been selected.

[22] M. Rejewski, 'Summary of our Methods for Reconstructing Enigma and Reconstructing Daily Keys, and of German Efforts to Frustrate Those Methods', in W. Kozaczuk, *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*, trans. C. Kasparek (London: Arms and Armour Press, 1984), 243.

[23] Rejewski's accounts of the work of the Polish cryptanalysts use 'message key' instead of the Bletchley term 'message setting'. See, for example, M. Rejewski, 'Jak Matematycy polscy rozszyfrowali Enigme' [How the Polish Mathematicians Broke Enigma], *Annals of the Polish Mathematical Society, Series II: Mathematical News*, 23 (1980), 1–28. (This article appears in an English translation by C. Kasparek as appendix D of Kozaczuk, *Enigma*; another translation, by J. Stepenske, appears in *Annals of the History of Computing*, 3 (1981), 213–34, under the title 'How Polish Mathematicians Deciphered the Enigma'.)

Operating Procedures

In order to decode the message, a recipient needs the wheel order, the *Stecker*, the *Ringstellung*, and the message setting. The most direct way to make the message setting available to the authorized recipient would be to make it an element of the daily key printed in the monthly tables. The operator would then simply look up the specified trigram for the day in question, and ensure that it was visible in the windows at the start of each message. This was the procedure used with the commercial form of Enigma.[24] But this method provided very weak security, reducing the problem of breaking a day's messages to that of solving a number of *substitution* ciphers.

The substitution cipher is an ancient and simple form of cipher in which the alphabet is paired with a 'scrambled' alphabet. For example:

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

THE ESSENTIAL TURING = GSV VHHVMGRZO GFIRMT

The great Polish cryptanalyst Marian Rejewski explained the weakness of enciphering a day's Enigma traffic at the same message setting:

> the first letters of all the messages . . . constituted an ordinary substitution cipher, a very primitive cipher easily soluable given sufficient material, and all the second letters of the messages . . . constituted another substitution cipher, and so on. These are not merely theoretical deliberations. It was in that very way that in France in 1940 we solved the Swiss Enigma cipher machine.[25]

The German armed forces employed more secure methods for making the message setting known to the intended recipient. The method adopted varied from service to service and from time to time, generally speaking with increasingly secure methods being used as time went on. From 1937 the German Navy used a particularly complicated method—although Turing did manage to break it. This method is described by Patrick Mahon in Chapter 5, which is an extract from Mahon's previously unpublished 'The History of Hut 8'. (Written in 1945, Mahon's 'History' was kept secret by the British and American governments until 1996.[26])

From the autumn of 1938 until May 1940 the German Army and Air Force used the following—as it turned out, highly insecure—method for sending the

[24] Rejewski, 'Remarks on Appendix 1 to British Intelligence in the Second World War by F. H. Hinsley', 79.

[25] Rejewski, 'How the Polish Mathematicians Broke Enigma', trans. Kasparek, 251.

[26] Mahon's 'The History of Hut 8' is in the US National Archives and Records Administration (NARA) in Washington, DC (document reference: RG 457, Historic Cryptographic Collection, Box 1424, NR 4685) and in the UK Public Record Office (document reference HW 25/2). A digital facsimile of the original typescript is available in The Turing Archive for the History of Computing <www.AlanTuring.net/mahon_hut_8>.

message setting to the recipient.[27] The sender would select two trigrams at random, say RBG and VAK. RBG is the message setting. VAK specifies the starting positions of the wheels that will be used not when encoding the message itself but when encoding the message setting prior to broadcasting it to the recipient. VAK would be broadcast to the recipient as part of an unencoded *preamble* to the encoded message. (The preamble could also include, for example, the time of origin of the message, the number of letters in the encoded message, and a group of letters called a *discriminant*, identifying the Enigma network to which the message belonged (e.g. Red).[28] The preamble might also contain an indication that the message was the second (or later) part of a two-part or multi-part message; see Mahon's discussion of 'forts' on pp. 278–9 below.)

The Indicator and Indicator Setting

Having selected the two trigrams, the sender would first set up VAK in the windows of his machine. He would then type RBGRBG. The group of six letters that lit up, say PRUKAC, is called the *indicator*. VAK is called the *indicator setting* (or '*Grundstellung*').[29] The indicator would be broadcast immediately before the enciphered message. The reason for sending the encipherment of RBGRBG, rather than simply of RBG, was to provide the recipient with a check that the message setting had been correctly received, radio reception sometimes being poor.

Once the sender had enciphered the message setting to form the indicator, he would set up RBG in the windows of his machine and type the plain text. Then the whole thing would be sent off to the recipient—preamble, indicator, and enciphered text.

The authorized recipient of the message would first rotate the wheels of his machine (already set up in accordance with the daily key) until VAK appeared in the windows. He would then type the indicator PRUKAC and the letters RBGRBG would light up at the lampboard. Now equipped with the message setting, he would set his wheels to RBG and retrieve the plain text by typing the encoded message.

[27] Rejewski, 'How the Polish Mathematicians Broke Enigma', trans. Kasparek, 265–6; Hinsley, *British Intelligence in the Second World War*, vol. iii, part 2, 949, 953.

[28] G. Bloch and R. Erskine, 'Enigma: The Dropping of the Double Encipherment', *Cryptologia*, 10 (1986), 134–41.

[29] The term 'indicator' is used by Mahon and Turing in the next chapter and is listed in 'A Cryptographic Dictionary', GC & CS (1944). ('A Cryptographic Dictionary' was declassified in 1996 (NARA document reference: RG 457, Historic Cryptographic Collection, Box 1413, NR 4559); a digital facsimile is available in The Turing Archive for the History of Computing <www.AlanTuring.net/crypt_dic_1944>.) However, the term 'indicator setting', which is from Welchman (*The Hut Six Story*, 36, 46) may not have been in use at Bletchley Park, where the German term *Grundstellung* (or 'Grund') was used (see e.g. pp. 272–3, below), as it was by the Poles (letter from Rejewski to Woytak, quoted on p. 237 of Kozaczuk, *Enigma*).

The method just described of selecting and making known the message setting is an example of what is called an *indicator system*.

3. The Polish Contribution, 1932–1940[30]

Unknown to GC & CS, the Biuro Szyfrów—the Polish Cipher Bureau—had already broken *Wehrmacht* Enigma, with assistance from the French secret service. The Biuro read the message traffic of the German Army regularly from 1933 to the end of 1938, and at other times during this period read the message traffic of other branches of the military, including the Air Force. Statistics gathered by the Biuro early in 1938 showed that, at that time, about 75 per cent of all intercepted Enigma material was being successfully decoded by the Biuro Szyfrów.

Towards the end of 1932 Rejewski had devised a method for reconstructing a day's message settings from the indicators, given about sixty messages sent on the day. He was helped by the fact that, in this early period, the indicator system was simpler than the later system just described. The daily key included an indicator setting *for the day*, e.g. VAK. The sender would choose his own message setting for each message, e.g. RBG. With the wheels in the positions specified in the daily key (VAK), he would type RBGRBG to produce the indicator. Then he would set the wheels to RBG and type the plain text of the message. The encoded message was sent prefaced by the preamble and the indicator—but, of course, there was no need to send the indicator setting.

Using information obtained from his attack on the indicators, Rejewski devised a method that enabled him to determine the internal wiring of wheels I–III (in those early days there were no additional wheels). This was one of the most far-reaching achievements in the history of cryptanalysis. Rejewski was assisted by the French secret service, whose agent Hans-Thilo Schmidt, a German employed in the cipher branch of the German Army, supplied photographs of two tables setting out the daily keys—*Stecker*, wheel order, *Ringstellung*, and the daily indicator setting—for September and October 1932. Rejewski describes this material as the 'decisive factor in breaking the machine's secrets'.[31]

[30] The sources for this section are: 'A Conversation with Marian Rejewski' (in Kozaczuk, *Enigma*), Rejewski's articles 'How the Polish Mathematicians Broke Enigma', 'Summary of our Methods for Reconstructing Enigma and Reconstructing Daily Keys, and of German Efforts to Frustrate Those Methods', 'The Mathematical Solution of the Enigma Cipher' (in Kozaczuk, *Enigma*), and 'Remarks on Appendix 1 to British Intelligence in the Second World War by F. H. Hinsley', together with Hinsley, vol. iii, part 2, appendix 30 'The Polish, French and British Contributions to the Breaking of the Enigma: A Revised Account'. (Appendix 30 replaces the sometimes very inaccurate appendix 1, 'The Polish, French and British Contributions to the Breaking of the Enigma', of Hinsley et al., *British Intelligence in the Second World War*, vol. i (London: Her Majesty's Stationery Office, 1979).

[31] Rejewski, 'How Polish Mathematicians Deciphered the Enigma', trans. Stepenske, 221.

In 1931 the French had attempted to interest the British in documents obtained by Schmidt, including operating manuals for German military Enigma. It is said that the British showed little interest, however, and declined to help the French meet the costs of obtaining them. It was not until 1936 that GC & CS began to study Enigma seriously. By the middle of 1939, Knox had discovered something like the Polish method for obtaining the message settings from the indicators (for German Army traffic).[32] However, he was unable to determine the internal wiring of the wheels. Without the wiring, it was impossible to use the method to decode the messages. GC & CS probably discovered a version of the same method that Rejewski had used to determine the wiring of the wheels, calling the method a 'Saga' (Mahon mentions it briefly on p. 278 of the next chapter). Knox is said to have outlined a 'more complicated version' of the Rejewski method at a meeting in Paris in January 1939.[33] However, he was never able to use this method to find the wiring of the wheels. This was because he was never able to discover the pattern of fixed wiring leading from the plugboard to the right-hand wheel via the entry plate (see Figure 4)—the 'QWERTZU', as he liked to call this unknown pattern, after the letters along the top row of the Enigma keyboard. This entirely humdrum feature of the military machine was what defeated Knox. Rejewski himself discovered the pattern by a lucky guess.

Once Rejewski had worked out the internal wiring of the wheels, he attacked the problem of how to determine the daily keys. This he solved early in 1933. At this stage, Rejewski was joined by Henryk Zygalski and Jerzy Różycki. Zygalski, Różycki, and Rejewski had graduated together from a course in cryptology that the Biuro Szyfrów had given in 1928–9. (Rejewski said later that it could have been the Biuro's fruitless efforts to break Enigma during 1928—the year in which the first messages were intercepted—that prompted the organization of the course at which the three were recruited.[34])

Now that the Polish cryptanalysts were able to find the daily keys on a regular basis, they needed access to Enigma machines in order to decipher the daily traffic. Using what Rejewski had found out concerning the wiring of the wheels, copies of the Wehrmacht Enigma were built by a Warsaw factory. Initially about half a dozen clerical staff were employed by the Biuro Szyfrów to operate the replica Enigmas. The clerical staff were 'put into a separate room, with the sole assignment of deciphering the stream of messages, the daily keys to which we soon began supplying'.[35] The number of replica Enigmas in use at the Biuro increased to about a dozen by mid-1934.

[32] Hinsley, *British Intelligence in the Second World War*, vol. iii, part 2, appendix 30, 951.

[33] Ibid.

[34] Letter from Rejewski to Richard Woytak, 15 Apr. 1979; the letter is printed in Kozaczuk, *Enigma*, 237–8.

[35] Rejewski, 'How the Polish Mathematicians Broke Enigma', trans. Kasparek, 261.

This state of affairs persisted until September 1938, when the German Army and Air Force abandoned the indicator system that Rejewski had broken in 1932. They switched to the indicator system described above: the indicator setting was no longer supplied in the tables giving the daily key, but was made up by the sender himself. Overnight the Poles' methods for determining the daily keys and message settings became useless. (In German Naval Enigma, the system broken by Rejewski had been abandoned in May 1937, when the complicated indicator system described by Mahon in the next chapter was adopted. Mahon outlines the Polish work on Naval Enigma to 1937.)

Within a few weeks of the September change, however, the Poles had devised two new methods of attack. One involved the use of perforated sheets of paper to determine the daily key, starting from a sufficient number of messages whose indicators displayed certain patterns of repeated letters. (Knox devised a similar method and was planning to use marks on photographic film rather than perforations, but was unable to put the method into practice without knowing the internal wiring of the wheels.[36]) The Poles' other method involved an electro-mechanical apparatus, designed by Rejewski and (on the engineering side) Antoni Palluth.[37] This was the *bomba* (plural 'bomby'), forerunner of the Bletchley Park bombe. How the bomba worked is explained in the next section. Six bomby were in operation by mid-November 1938.

The bomby and the perforated sheets depended on the fact that the indicator was formed by enciphering the message setting *twice* (e.g. enciphering RGBRGB rather than simply RGB). If the indicator system were changed so that the message setting was enciphered only once, the bomby and the perforated sheets would become unusable. This is precisely what was to happen in May 1940. Well before this, however, the bomby became overwhelmed by other changes designed to make Enigma more secure.

In December 1938 the Germans introduced the two extra wheels, IV and V. The Poles were able to determine the internal wiring of the new wheels by the method used in 1932 (thanks to the fact that one Enigma network—the intelligence service of the Nazi party—had not adopted the indicator system that came into force on other networks in September 1938 and was still using the system that the Poles could break by their earlier methods). But the material resources of the Biuro Szyfrów were insufficient to enable the Poles to cope with the increase in the number of wheel orders that the two new wheels produced. Where previously there had been only six possible wheel orders, there were now sixty. In order to investigate the new wheel orders, at least thirty-six replicas of each new wheel were required. The factory could not produce replicas fast enough.

[36] Hinsley, *British Intelligence in the Second World War*, vol. iii, part 2, appendix 30, 951.

[37] Rejewski, 'How the Polish Mathematicians Broke Enigma', 267.

Work with the perforated sheets was affected in the same way. The drawback of the sheet method had always been that the manufacture of a single sheet required the cutting of about 1,000 tiny perforations in exactly the right positions, with twenty-six sheets being required for each possible wheel order. Suddenly a huge number of additional sheets was required.

The result of the addition of the new wheels was that the Poles were able to read German Army and Air Force messages on only those days when it happened that wheels I, II, and III were in the machine—on average one day in ten.

Pyry and After

In July 1939 the Poles invited members of the British and French intelligence services to a meeting at Pyry near Warsaw. Denniston and Knox represented GC & CS. At this meeting, Rejewski relates, 'we told everything that we knew and showed everything that we had'—a replica Enigma, the bomba, the perforated sheets, and of course the all-important internal wiring of the wheels, which Knox still had not been able to work out.[38] Without the Poles, Knox and Turing might not have found out the wiring of the wheels until May 1940, when the British captured several intact Enigma machines from the German Army in Norway.

Knox's first question to the Poles was 'What is the QWERTZU?'[39] The answer was almost a joke—the connections were in *alphabetical* order, with the A-socket of the plug-board connected to the first terminal inside the entry plate, the B-socket to the second, and so on. Knox was ecstatic to know the answer at last, chanting in a shared taxi 'Nous avons le QWERTZU, nous marchons ensemble' ('We have the QWERTZU, we march along together').[40]

At Pyry the Poles also undertook to supply their British and French allies with two replica Enigma machines. The replica destined for GC & CS was couriered from Paris to London on 16 August 1939 by two men, Gustave Bertrand, head of the codebreaking section of the French Intelligence Service, and 'Uncle Tom', a diplomatic courier for the British Embassy in Paris. On the platform of Victoria Station they handed the machine over to Admiral Sinclair's deputy, Colonel Stewart Menzies. Menzies, on his way to an evening engagement, was dressed in a dinner jacket and he sported the rosette of the Légion d'Honneur in his buttonhole. *Accueil triomphal*—a triumphant welcome, Bertrand declared.[41]

Following the invasion of Poland, Rejewski and his colleagues moved to France. By January 1940 GC & CS, with its superior resources, had produced two complete sets of perforated sheets. The Poles received one of the sets in instalments. Turing delivered some of the sheets himself.

[38] Ibid. 269.

[39] Ibid. 257; P. Twinn, 'The *Abwehr* Enigma', in Hinsley and Stripp (eds.), *Codebreakers*, 126.

[40] Twinn, 'The *Abwehr* Enigma', 126–7.

[41] G. Bertrand, *Enigma, ou la plus grande énigme de la guerre 1939–1945* (Paris: Plon, 1973), 60–1.

Rejewski recollected: 'We treated [Turing] as a younger colleague who had specialized in mathematical logic and was just starting out in cryptology. Our discussions, if I remember correctly, pertained to the commutator [plugboard] and plug connections (Steckerverbindungen) that were Enigma's strong point.'[42] Little did Rejewski know that Turing had already devised the brilliant method of dealing with the *Steckerverbindungen* on which the British bombe was based.

For several months the British and the Poles worked in cooperation. The first break of wartime traffic since September 1939 was achieved by the Poles in mid-January 1940, followed a few days later by further breaks at GC & CS. During the period of fruitful collaboration that ensued, the Poles with their lesser resources were responsible for about 17 per cent of the daily keys broken.

Then, in May 1940, everything changed. The new indicator system introduced by the German Army and Air Force on 1 May made the perforated sheets useless for all networks except one, Yellow, which continued to employ the old system. Even Yellow, an inter-services key in use during the Norway campaign, went out of service on 14 May.[43] The change of indicator system and the German occupation of France effectively ended the attack on Enigma by the exiled Biuro Szyfrów.

The British were able to continue reading German Air Force messages (from 20 May) by means of methods developed at GC & CS which exploited the bad habits of some German Enigma operators. One was the habit of enciphering the message setting at the position that the wheels happened to be in at the end of the previous message, or at a closely neighbouring position (obtained e.g. by lazily turning only one wheel some small number of clicks).

From the summer of 1940 the codebreakers at GC & CS began to receive assistance from Turing's radically redesigned version of the Polish bomba.

4. The Polish Bomba

Origin of the Name 'Bomba'

In Chapter 5, Mahon says that the British bombe 'was so called because of the ticking noise it made, supposedly similar to that made by an infernal machine regulated by a clock' (p. 291). This story was well entrenched among Bletchleyites. The need-to-know principle meant that few were aware of the Polish bomba. Similarly, the explanation that circulated at Bletchley Park of why certain patterns, involving repetitions of letters at the same places, were known as 'females' took no account of the fact that the terminology had been borrowed

[42] Quoted in Kozaczuk, *Enigma*, 97. On Turing's visit to the Poles, see ibid 96–7; Welchman, *The Hut Six Story*, 220; and R. Erskine, 'Breaking Air Force and Army Enigma', in Erskine and Smith, *Action This Day*, 54.

[43] Erskine, 'Breaking Air Force and Army Enigma', 55.

from the Poles. The equivalent Polish term 'samiczki', meaning 'females', was quite likely the result of a play on words, 'samiczki' being used as short for a Polish phrase meaning 'the same places.'[44]

Why the Poles chose the name 'bomba' seems not to have been recorded. Rejewski's only comment was that the name was used 'for lack of a better idea'.[45] As well as meaning 'bomb', 'bomba' is the Polish word for a type of ice-cream dessert—*bombe* in French. Tadeusz Lisicki, who corresponded with Rejewski during the years before the latter's death in 1980, is quoted as saying: 'The name "bomba" was given by Różycki... [T]here was in Warsaw [an] ice-cream called [a] bomba... [T]he idea [for] the machine came while they were eating it.'[46]

A different story is told in recently declassified American documents. As explained later in this section, the bomba is required to stop immediately it detects a certain feature. How this was achieved by the Polish engineers is not known for sure. The American documents suggest that the stopping mechanism involved the dropping of weights, and the claim is made that this is how the name arose.

> [A] bank of Enigma Machines now has the name 'bombe'. This term was used by the Poles and has its origin in the fact that on their device when the correct position was reached a weight was dropped to give the indication.[47]
>
> When a possible solution was reached a part would fall off the machine onto the floor with a loud noise. Hence the name 'bombe'.[48]

It is not implausible that falling weights were used to disengage the bomba's drive mechanism (a printer designed by Babbage as part of his Difference Engine used a similar idea). However, the two American documents in question were written some years after Rejewski and his colleagues destroyed all six bomby in 1939[49] and neither cites a source for the claim quoted (the documents are dated 1943 and 1944). Moreover, both documents contain inaccurate claims concerning the Polish attack on Enigma (for example, that the bomba was 'hand operated', and that the military Enigma machine had no plug-board until 'about 1938').[50] The sketch of the bomba that accompanies Rejewski's 'The Mathematical Solution

[44] Kozaczuk, *Enigma*, 63.

[45] Rejewski, 'How the Polish Mathematicians Broke Enigma', 267.

[46] Tadeusz Lisicki quoted in Kozaczuk, *Enigma*, 63.

[47] Untitled typescript dated 11 Oct. 1943 (NARA, document reference RG 457, Historic Cryptographic Collection, Box 705, NR 4584), 1.

[48] 'Operations of the 6312th Signal Security Detachment, ETOUSA', 1 Oct. 1944 (NARA, document reference: RG 457, Historic Cryptographic Collection, Box 970, NR 2943), 5. (Thanks to Ralph Erskine for drawing my attention to this quotation and to Frode Weierud for sending me a copy of the document.)

[49] Rejewski, 'Remarks on Appendix 1 to British Intelligence in the Second World War by F. H. Hinsley', 81.

[50] Untitled typescript dated 11 Oct. 1943, 2; 'Operations of the 6312th Signal Security Detachment, ETOUSA', 5.

of the Enigma Cipher' shows no system of falling weights—although nor is an alternative system for stopping the bomba depicted.[51]

Simple Enigma and a Mini Bomba

Let us suppose, for purposes of illustration, that we are dealing with an imaginary, highly simplified, version of the Enigma machine called Simple Enigma. Simple Enigma has one wheel rather than three and no plug-board; in other respects it is the same as a full-scale Enigma.

Suppose that we have a message to decode beginning NYPN... Suppose further that we have a *crib*. A crib is a series of letters or words that are thought likely to occur in the plain language message that the cipher text encrypts. Say we have good reason to believe that the first and fourth letters of the plain text are both E (perhaps a prisoner gasped out the first four letters of the plain text before he died, but his second and third gasps were inaudible). We will use a machine to help us find the message setting—i.e. the rotational position of the wheel at which the sender began typing the message.

Our code-breaking machine consists of two replicas of the Simple Enigma machine plus some additional devices. There is a mechanism for holding down any selected key at the keyboards of the replicas, thereby keeping the current flowing from key to wheel. The wheel of each replica can be locked in step with the other, and there is an electric motor that will click the wheels round in unison through their twenty-six rotational positions, one position at a time. Additional circuitry bridging the two lampboards detects whether a selected letter—E, for example—lights up simultaneously at each lampboard. A switch or relay is wired in such a way that if the selected letter does light simultaneously, the electric motor is turned off, with the result that the wheels stop turning at exactly the position that caused the simultaneous lighting of the letter. This is called a 'stop'.

Assuming that the crib is correct, we know that if the intended recipient of the message sets the wheel of Simple Enigma to the message setting and types the first letter of the cipher text, N, the letter E will light up at the lampboard. The recipient will then type the next two letters of the cipher text, YP, causing unknown letters to light, followed by the fourth letter of the cipher text, N, which will cause E to light up again. Each time the recipient presses a key at the keyboard, the wheel advances one click. So the position of the wheel at which the fourth letter of the cipher text decodes as E is three clicks on from the position at which the first letter of the cipher text decodes as E. This is expressed by saying that these two positions are at a *distance of three* from each other. What we want our codebreaking machine to do is to search through the twenty-six possible positions of the wheel, looking for a position p that satisfies these two conditions:

[51] Kozaczuk, *Enigma*, figure E-8, 289.

1. At position p, keying N causes E to light;
2. At position $p + 3$ (i.e. the position three on from p), keying N again causes E to light.

We set up the codebreaking machine to perform this search by turning one of the two identical wheels so that it is three positions ahead of the other. For example, we might turn the wheel on the right so that, of the twenty-six letters marked around its ring, Z is uppermost, and then position the wheel on the left three clicks further on, i.e. with C uppermost. The two wheels are then locked together so that they will maintain their position relative to one another while the motor rotates them. The locked wheels are described as being at an *offset* of three clicks.

Next we set up the additional circuitry at the lampboards so that the simultaneous lighting of the letter E at each board will produce a stop. Finally, we clamp down the N-key at each of the two keyboards and start the electric motor.

The motor turns the wheels from position to position. If all goes well, a point is reached where E lights at both boards and the machine stops. If at that stage the wheels have not yet completed a full revolution, we note the position at which the stop occurred and then start the motor again, since there might be more than one position at which conditions 1 and 2 are jointly satisfied. (If, after a complete revolution, there are no stops, our crib was incorrect.)

If a complete revolution brings only one stop, then the position of the right-hand wheel of the pair must be the position at which the sender began encoding the message. We pass this setting to a clerk sitting at another replica of the Simple Enigma, who turns the wheel to that position and keys in the cipher text, producing the plain text at the lampboard. If there were several stops, then the clerk has to try each of the possible settings in turn until one is found that yields German at the lampboard.

Notice that we have not discovered the actual message setting—the letter visible in the window of the sender's machine at the start of typing the message (and enciphered to form the indicator). Which letter is visible in the window depends on how the sender has positioned the ring around the 'core' of the wheel. Leaving the core in one position, the operator could make any one of the twenty-six letters appear in the window by twisting the ring around the core. What we have found is the position *of the wheel core* at the start of the message. At GC & CS this was called the 'rod-position' of the wheel. The rod-position is all we need to be able to decipher the message.

Of course, with only twenty-six positions to search through, there is hardly any need for the electric motor, the detector circuitry at the lampboards, and so forth, because one could quite quickly conduct the search simply by turning the wheels of two replica machines manually. However, the additional equipment is certainly necessary when it is the full-scale Enigma machine that is being attacked, since the existence of three wheels and six possible wheel orders

means that one must search through not 26 but $6 \times 26 \times 26 \times 26 = 105,456$ possible positions. (This figure ignores the small complications introduced by double-notching and by the extra movement of the middle wheel described above.)

The Actual Bomba

The Polish bomba was a more complicated version of the mini bomba just described. It consisted in effect of six replica Enigma machines, with six sets of duplicates of wheels I, II, and III—eighteen wheels in all. Each of the six replica Enigmas in a single bomba was usually set up with the same wheel order, for example III/I/II. The wheels used in a bomba had no rings (and so no notches for producing a 'turnover' of the adjacent wheel).

The six replica Enigmas were linked in pairs to form three double-Enigmas—just as in the example of the mini bomba, where two Simple Enigmas are linked to form a double Simple Enigma. Each of these double-Enigmas included three pairs of wheels and equipment equivalent to two keyboards and two lampboards. The complete bomba consisted of the three double-Enigmas plus the electric motor, a mechanism for detecting simultaneities and producing stops, and arrangements for holding constant the letter going into each double-Enigma.

At this point it may be helpful to repeat that the first, or outermost, of the three wheels in an Enigma machine—the wheel linked directly to the keyboard and plug-board and which moved once with every key-stroke—was always the right-hand member of the trio. For example, if the wheel order is I/II/III, it is wheel III that is the outermost of the three wheels.

As in the mini bomba, the identical wheels of a double-Enigma were locked in step, sometimes with one member of a pair a number of positions ahead of the other member. For example, the two IIIs might be locked in step at an offset of three clicks (as above), while the two IIs are locked in step with no offset, and likewise the two Is.

The corresponding wheels of different double-Enigmas in the same bomba were also locked in step with one another. For example, the locked pair of III wheels of one double-Enigma might be locked in step (at an offset of twelve clicks, say) with the locked pair of III wheels of another double-Enigma.

Once all the wheels were appropriately linked, the electric motor would be started and the bomba's six replica Enigmas would move in synchronization, each passing through $26 \times 26 \times 26$ positions. This took about two hours, each outer wheel moving through 676 revolutions, each middle wheel through 26 revolutions, and each left-hand wheel through one revolution. In the space of roughly two hours, the bomba could do the same work that would occupy a human computer for about 200 hours.[52]

[52] See p. 40.

The Indicator Method

In the previous example, we imagined using a mini bomba to discover wheel positions consistent with a crib concerning the first and fourth letters of the cipher text. The method employed by the Poles was different and did not involve text-cribbing (although the method that Turing would later devise for the British bombe did). The Poles focused on the *indicator* (to recapitulate: the six-letter group preceding the cipher text and produced by enciphering the message setting twice, at an indicator setting that the sender broadcast 'in clear' as part of the preamble to the message).

In a proportion of the intercepted messages, the first and fourth letters of the indicator would be the same, as for example in the indicator WAHWIK.[53] Since an indicator is produced by typing a three-letter message setting twice, the first and fourth letters of any indicator both encode the same letter as each other. This is true also of the second and fifth letters of any indicator, and the third and sixth. So both the occurrences of W in WAHWIK encode the same letter; and moreover three clicks of the right-hand wheel separate the two positions at which W encodes this unknown letter.

Let me use 'p_R' when referring to a position of the Enigma's right-hand wheel, and similarly 'p_M' in the case of the middle wheel and 'p_L' in the case of the left-hand wheel. We could attempt to use the bomba to search for rod-positions p_L, p_M, and p_R such that at position p_R and position $p_R + 3$, W encodes the same letter. As I will explain, this is not in fact an effective way to proceed, but in order to get the feel of the bomba, let's briefly consider how to carry out this search.

We select one of the double-Enigmas, pick a wheel order, say I/II/III, and put the three pairs of wheels into this order. We then lock the right-hand pair, the IIIs, in step at an offset of three (just as in the example of the mini bomba). The wheels in the middle pair (the IIs) are locked in step at the same position as one another, and likewise the wheels in the left-hand pair (the Is). Finally, we set the detector circuits to produce a stop whenever the same letter—any letter—lights simultaneously in both Enigmas. (The remaining two double-Enigmas are not needed for this search.) The motor is switched on and each replica Enigma moves through its $26 \times 26 \times 26$ positions. Any stops give pairs of positions, three clicks of the right-hand wheel apart, at which typing W produces the same letter at the lampboard. Another five runs of the bomba are required to explore all six wheel orders. (Alternatively we might use all three double-Enigmas, each

[53] The indicators and indicator settings used in this example are adapted from p. 266 of Kasparek's translation of Rejewski's 'Jak Matematycy polscy rozszyfrowali Enigme' in Kozaczuk, *Enigma*. The present description of the bomby has been reconstructed from Rejewski's rather compressed account appearing on that page. Unfortunately, Stepenske's translation of these same paragraphs in the *Annals of the History of Computing* is marred by an error that seriously affects the sense. The phrase that Stepenske translates 'by striking key W three times in a row, the same lamp would light' (p. 226) should be translated 'if key W is struck the same lamp will light again after three more strokes'.

with a different wheel order, so enabling the bomba to explore three wheel orders simultaneously. In this case only two runs of the bomba are necessary to cover all the possible wheel orders.)

Notice that an assumption is being made here concerning 'turnovers'. As previously explained, the movement of the right-hand wheel of the Enigma machine at some point causes the centre wheel to turn forward one click; and the movement of the centre wheel at some point causes the left-hand wheel to advance one click. The positions at which these turnovers occur are determined by the *Ringstellung*. In locking the pair of II wheels (the middle wheels) of the double-Enigma together in the *same* position as one another, we are assuming that, as the sender's machine lights up the letters WAHWIK, no movement of the middle wheel occurs during the three clicks forward of the right-hand wheel that lie between the production of the first and second occurrences of W. And in locking the left-hand wheels of the double-Enigma together in the same position, we are making the same assumption about the left-hand wheel of the sender's machine.

Of course, these assumptions might be wrong, in which case the search will fail. This is no less true in the case of the full-blooded search described below involving three indicators. However, the assumption that only the right-hand wheel moves in the course of typing a group of six letters is true much more often than not, and so searches based on this assumption will, other things being equal, succeed much more often than not.

The problem with the method of searching just described is that it would typically produce excessively many stops—many triples of positions p_L, p_M, p_R are liable to satisfy the rather mild constraint that W encodes the same letter at both p_R and $p_R + 3$. It would take the clerk who tries out each stop by hand on a further replica Enigma far, far too long to winnow out the correct wheel positions. It is necessary to find additional indicators from the same day's traffic that can be used to narrow the focus of the bomba's search. Here is what the Poles actually did.

In order to put a bomba to work effectively, it is necessary to find in a single day's traffic (i.e. traffic encoded with the same wheel order and *Stecker*) three messages whose indicators exhibit the following patterns of repetitions. One indicator must display the pattern just discussed—the same letter repeated at the first and fourth positions, as in the example

WAHWIK.

A second indicator must have the selfsame letter that is at positions 1 and 4 in the first indicator at its second and fifth positions, as in

DWJMWR.

A third indicator must have that same letter at its third and sixth positions, as in

RAWKTW.

The Poles called these patterns 'females' (see above). At Bletchley Park the three patterns were referred to as a 1–4 female, a 2–5 female, and a 3–6 female respectively. It is because this indicator system admits three types of female that the bomba contains three double-Enigmas, each one utilizing the information contained in one of the three females.

Let the position of the right-hand wheel when the first letter of the first indicator was produced be p_R and the position of the right-hand wheel when the first letter of the second indicator was produced be q_R, and likewise r_R in the case of the third indicator. We know from the patterns of repeated letters in the indicators that:

> Keying W produces a simultaneity at p_R and $p_R + 3$ (i.e. at p_R and $p_R + 3$ the same letter lights). Keying W produces another simultaneity at $q_R + 1$ and $q_R + 4$ (possibly involving a different letter at the lampboard). Keying W produces a third simultaneity at $r_R + 2$ and $r_R + 5$.

In fact we know more than this. A rich source of information has not yet been used—the indicator settings which appear in clear in the preambles to the messages. Suppose these are as follows.

indicator setting	*indicator*
RTJ	WAHWIK
DQY	DWJMWR
HPB	RAWKTW

Without the wheel order and the *Ringstellung* for the day in question, which of course we do not yet possess, the indicator setting cannot be used straightforwardly to decode the indicator. Nevertheless, the indicator settings are far from useless to us, because they contain information about the *relative* positions of the wheels when the indicators were produced; and using this information, we can deduce the relationship between p_R, q_R, and r_R.

The right-hand letter of each indicator setting specifies the position of the right-hand wheel when the encryption—or equivalently the decryption—of each message setting begins. Similarly, the middle letter specifies the position of the middle wheel when the encryption of the message setting begins, and the left-hand letter the position of the left-hand wheel. Picture the letters of the alphabet arranged evenly around the circumference of a circle, as on the ring of a wheel. The right-hand letter of the second indicator setting, Y, is fifteen letters further on than the right-hand letter of the first indicator setting, J. Therefore the position of the right-hand wheel at which the first letter of the second indicator was produced, q_R, is fifteen clicks on from the position at which the first letter of the first indicator was produced, p_R:

$$q_R = p_R + 15$$

The right-hand letter of the third indicator setting, B, is eighteen letters on from J (JKLMNOPQRSTUVWXYZAB). Therefore the position of the right-hand wheel at which the first letter of the third indicator was produced, r_R, is eighteen clicks on from p_R:

$$r_R = p_R + 18$$

Inserting this additional information into the above statement about simultaneities gives:

> Keying W produces a simultaneity at p_R and $p_R + 3$; another simultaneity at $(p_R + 15)+1$ and $(p_R + 15)+ 4$; and a third simultaneity at $(p_R+18)+2$ and $(p_R+18) + 5$.

Or more simply:

> Keying W produces a simultaneity at p_R and $p_R + 3$; another simultaneity at $p_R + 16$ and $p_R + 19$; and a third simultaneity at $p_R + 20$ and $p_R + 23$.

Now we have a much stronger constraint on p_R and can use the bomba to search for p_R and the accompanying positions of the other wheels in the expectation that the number of stops will be small enough to be manageable.

Using the Bomba

The bomba is set up for the search as follows. The stopping mechanism is arranged to produce a stop whenever the eighteen wheels move into a configuration that causes a simultaneity at each of the three double-Enigmas at once. The three simultaneities need not involve the same lampboard letter as each other. W is input continuously into the Enigmas.

One double-Enigma is set up as above: the wheel order is I/II/III, the III wheels are locked together at an offset of three, and the other pairs of wheels are locked with no offset (the assumption being, as before, that neither the middle nor the left-hand wheel of the sender's machine moved during the production of WAH-WIK). Call this double-Enigma's III wheels $\mathbf{l}_1$ and $\mathbf{r}_1$ (for the left and right members of the pair); $\mathbf{r}_1$ is three clicks ahead of $\mathbf{l}_1$.

The second double-Enigma is set up with the same wheel order. Call its III wheels $\mathbf{l}_2$ and $\mathbf{r}_2$. $\mathbf{l}_2$ is locked in step with $\mathbf{l}_1$ at an offset of 16, and $\mathbf{r}_2$ is locked in step with $\mathbf{l}_2$ at an offset of 3 (so $\mathbf{r}_2$ is nineteen clicks ahead of $\mathbf{l}_1$). As with the first double-Enigma, the II wheels are locked in step with no offset, and likewise the Is. The third double-Enigma is also set up with wheel order I/II/III. Its III wheels are $\mathbf{l}_3$ and $\mathbf{r}_3$. $\mathbf{l}_3$ is locked in step with $\mathbf{l}_1$ at an offset of 20, and $\mathbf{r}_3$ is locked in step with $\mathbf{l}_3$ at an offset of 3 (so $\mathbf{r}_3$ is twenty-three clicks ahead of $\mathbf{l}_1$). Again, the II wheels are locked in step with no offset, and the same for the Is.

Next, each double-Enigma must have its pair of II wheels suitably synchronized with those of its neighbours, and similarly its I wheels. This is achieved as in

the case of the III wheels by making use of the information contained in the indicator settings about the relative positions of the wheels of the sender's machine when the indicators were produced.

The middle letter of the second indicator setting, Q, is twenty-three places ahead of the middle letter of the first indicator setting, T. So the middle wheels of the second double-Enigma—the IIs—are locked in step with the middle wheels of the first at an offset of 23. The middle letter of the third indicator setting, P, is twenty-five places ahead of the middle letter of the second indicator setting, Q, so the middle wheels of the third double-Enigma are locked in step with the middle wheels of the second at an offset of 25. The left-hand letter of the second indicator setting, D, is twelve places ahead of the left hand letter of the first indicator setting, R, so the left-hand wheels of the second double-Enigma—the Is—are locked in step with the left-hand wheels of the first double-Enigma at an offset of 12. Finally, the left-hand letter of the third indicator setting, H, is four places ahead of the left-hand letter of the second indicator setting, D, so the left-hand wheels of the third double-Enigma are locked in step with the left-hand wheels of the second at an offset of 4.

The motor is switched on. As before, the stops that are produced during a run through all $26 \times 26 \times 26$ positions are noted and then tested by a clerk. If none works, it is necessary to set up the bomba again with a different wheel order. Six runs are required to search through all the wheel orders—approximately twelve hours of bomba time in total. By running six bomby simultaneously, one for each wheel order, the Poles reduced the search time to no more than two hours.

The clerk at the replica Enigma tests the various positions at which the stops occurred. He or she eventually finds one that deciphers each indicator into something of the form XYZXYZ. The cryptanalysts now know the message settings and the rod-positions of the wheels at which the message settings were enciphered.

To use the message settings to decode the messages it is necessary to know the *Ringstellung* (since a message setting XYZ could specify any one of the $26 \times 26 \times 26$ positions, depending on the position of the ring). However, the *Ringstellung* lies only a step away. It can be deduced by comparing the rod-positions of the wheels at which the first letter of any of the indicators was produced with the corresponding indicator setting.

For example, if the *Ringstellung* is set correctly, then what should appear in the windows when the wheel cores lie in the positions at which the first W of WAHWIK was produced is RTJ. Since these rod-positions are know, it is a simple matter to take replicas of the wheels and to twist the rings until the letters R, T and J are uppermost at these rod-positions. Once the rings are correctly positioned, a wheel's ring setting is given by the position of the ring against the embossed index mark on the wheel core: whatever letter lies against the index

mark is the ring setting for that wheel. The complete *Ringstellung* is the trigram consisting of the letter for each wheel arranged in the wheel order for the day.

Now the messages can be decoded on a replica Enigma, as can other intercepted messages with the same wheel order and *Ringstellung*.

The Plug-Board Problem

It remains to explain how the permutations introduced by the plug-board were dealt with. In the military Enigma machine, the plug-board or stecker-board lay in the path both of current flowing from the keyboard to the wheels and of current flowing from the wheels to the lampboard (see Figure 4). Not every keyboard key was affected by the plug-board. When the bomba first came into operation, the Germans were using the plug-board to scramble between ten and sixteen of the twenty-six keys (in effect by swapping the output wires of pairs of keys). The remaining keys were unaffected, being 'self-steckered'.

It was specified in the daily key which (keyboard) keys were to be affected on any given day and how the affected (keyboard) keys were to be paired up. For example, suppose the daily key says that T and K are to be 'steckered'. The operator connects together the plug-board sockets labelled T and K (by means of a cord with a plug at each end). The result of this extra twist is that pressing the T-key at the keyboard produces the effect at the wheels which pressing the K-key would have produced had there been no scrambling of the letters at the plug-board. Likewise pressing the K-key produces the effect which pressing the T-key would have produced in the unsteckered case.

The plug-board comes into play a second time, in between the wheels and the lampboard. If K lights up in the steckered case, then the selfsame output from the wheels would have caused T to light up had T been one of the letters unaffected by the plug-board. Likewise if T lights up, the output would have caused K to light up had K been unaffected by the plug-board.

The bomba took no account at all of *Stecker*. If the females in the chosen indicators had been produced without interference from the plug-board (i.e. if all the letters in the indicators were self-steckered), then the bomba could produce the correct message setting. But if stecker-substitutions were involved, the bomba would be looking for the wrong thing. Returning to the above example, it would not be W that produces simultaneities at p_R and $p_R + 3$, and so on, but the letter to which W happened to be steckered; and so the bomba's search would fail.

The success of the bomby depended on the fact that, with between ten and sixteen letters unaffected by the plug-board, there was a reasonable chance of the day's traffic containing three indicators unpolluted by *Stecker* and displaying the requisite females.

Once the wheel order and *Ringstellung* had been discovered, messages could be deciphered using a replica Enigma on which all letters were self-steckered. The

result would be German words peppered with incorrect letters produced by plug-board substitutions. These incorrect letters gave away the plug-board connections of the sender's machine.

On 1 January 1939 the Germans increased the number of letters affected by *Stecker* (from between five and eight pairs of letters to between seven and ten pairs). The effectiveness of the bomba—already severely compromised by the introduction of wheels IV and V in December 1938—diminished still further.

5. The Bombe and the Spider

At Pyry, Knox observed that the indicator system exploited by the bomba might 'at any moment be cancelled'—as did indeed happen in May 1940 (see above).[54] It was clear to Knox that even if the problems engendered by the increases in the number of wheels and the number of steckered letters could be solved, the modified bomba might become unusable overnight. After the Warsaw meeting Knox and Turing considered the possibility of using a bomba-like machine to attack not the indicators but the message text itself, via cribs.[55] The decision was taken to build a flexible machine that could be used both in the Polish manner against the indicators and also with cribs.

Turing was responsible for the logical design of the machine—the 'bombe'. He passed his design to Harold 'Doc' Keen at the factory of the British Tabulating Machine Company in Letchworth. Keen handled the engineering side of the design. Notes dated 1 November 1939 signed by Knox, Turing, Twinn, and Welchman refer to 'the machine now being made at Letchworth, resembling but far larger than the Bombe of the Poles (superbombe machine)' and state: 'A large 30 enigma bomb [*sic*] machine, adapted to use for cribs, is on order and parts are being made at the British Tabulating Company.'[56]

Knox himself appears to have made little or no contribution to the design and development of the bombe. His greatest achievements during the war were breaking the versions of Enigma used by the Italian Navy and by the *Abwehr*, the secret intelligence service of the German High Command.[57] He died in February 1943.

In its mature form the bombe contained thirty-six replica Enigmas. (The replicas were made at Letchworth and in Chapter 6 Turing refers to them as 'Letchworth Enigmas'.) The intricate bombe contained some ten miles of wire and one million soldered connections. Enclosed in a cabinet, the bombe stood 6 feet 6½ inches tall (5 feet 10 inches without its 8½ inch castors), 7 feet 3¾ inches

[54] Hinsley, *British Intelligence in the Second World War*, vol. iii, part 2, appendix 30, p. 954.

[55] Ibid.

[56] 'Enigma—Position' and 'Naval Enigma Situation', notes dated 1 Nov. 1939 and signed by Knox, Twinn, Welchman, and Turing. Both notes are in the Public Record Office (document reference HW 14/2).

[57] Batey, 'Breaking Italian Naval Enigma'; Twinn, 'The *Abwehr* Enigma'.

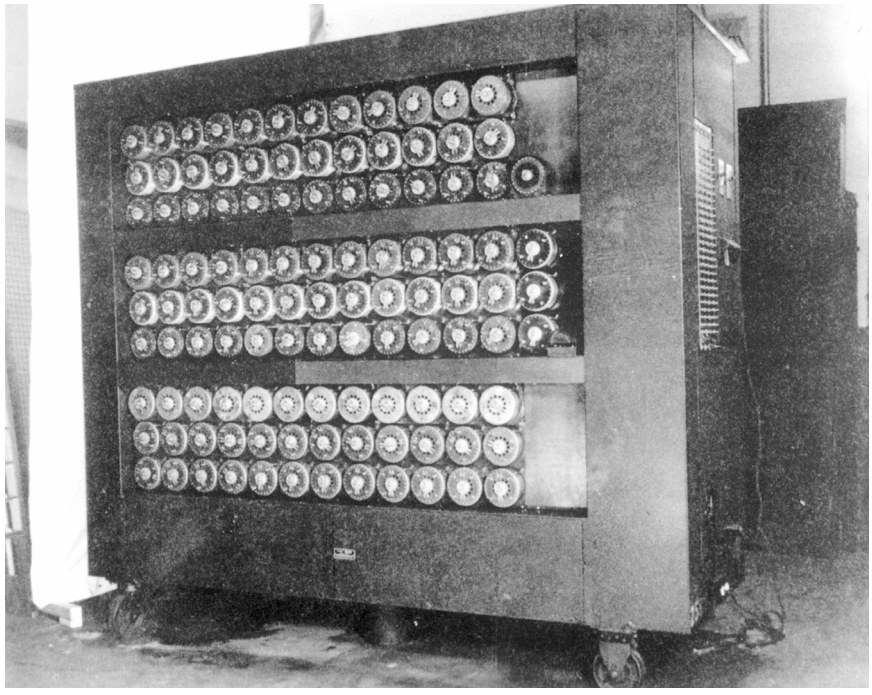

Figure 7. A Bletchley bombe.

Source: Science and Society Picture Library, National Museum of Science and Industry.

long, and 2 feet 7 inches deep.[58] From the front, nine rows of rotating drums were visible. Each drum mimicked a single Enigma wheel.[59] The drums (which were almost 5 inches in diameter and $1\frac{3}{4}$ inches deep) were removable and could be arranged to correspond to different wheel orders. Colour-coding was used to indicate which wheel, e.g. IV, a particular drum mimicked. The drums were interconnected by means of a large panel at the rear of the bombe (a panel that 'almost defies description—a mass of dangling plugs on rows of letters and numbers', according to one WRN operator; Mahon says that when viewed from the rear, the bombe appeared to consist 'of coils of coloured wire, reminiscent of a Fair Isle sweater' (p. 291, below)).[60] The replica Enigmas in the bombe could be connected together arbitrarily, according to the demands of whatever crib was being run.

[58] 'Operations of the 6312th Signal Security Detachment, ETOUSA', 60. (Thanks to John Harper for additional information.)

[59] 'Operations of the 6312th Signal Security Detachment, ETOUSA', 67.

[60] D. Payne, 'The Bombes', in Hinsley and Stripp (eds.), *Codebreakers*, 134. The coils of wire described by Mahon were probably red in colour. Red wire and very rarely black wire were used by the Letchworth bombe factory (letter from John Harper to Copeland (25 Feb. 2003), reporting interviews with engineers who worked on the bombes at the Letchworth factory).

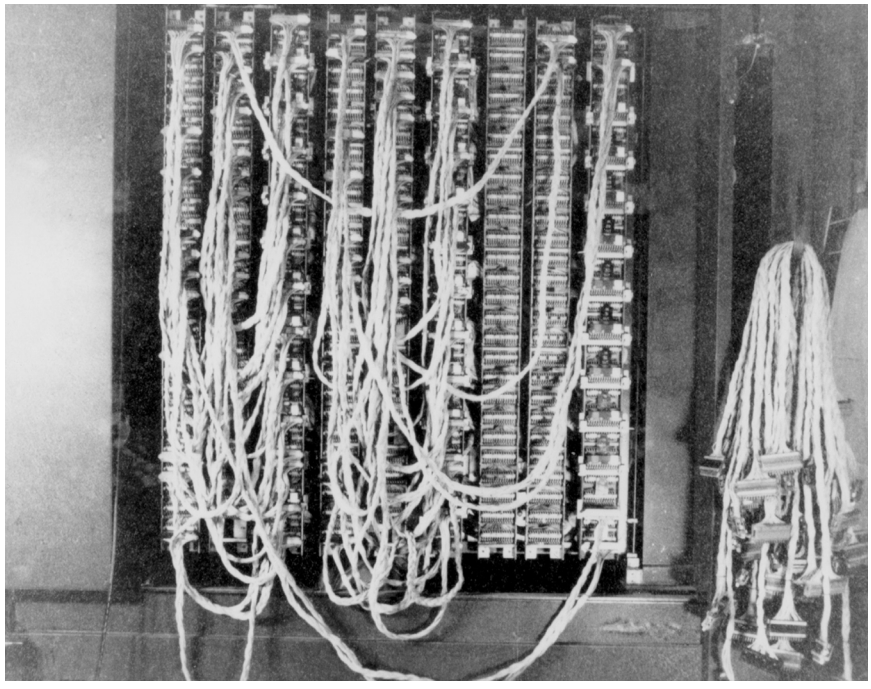

Figure 8. Rear panel of a bombe.

Source: Science and Society Picture Library, National Museum of Science and Industry.

Cribs

Cribs resulted both from the stereotyped nature of the messages sent by the Germans and from the thoughtlessly insecure habits of some operators. For example, weather stations regularly sent messages beginning in stereotyped ways, such as 'WETTER FUER DIE NACHT' ('Weather for the night') and 'ZUSTAND OST WAERTIGER KANAL' ('Situation Eastern Channel'). In Chapter 5 Mahon relates how a certain station transmitted the confirmation 'FEUER BRANNTEN WIE BEFOHLEN' each evening ('Beacons lit as ordered').

The position of the cribbed phrase within the cipher text could often be found by making use of the fact that the Enigma never encoded a letter as itself. The cryptanalyst would slide a suspected fragment of plain text (e.g. ZUSTAND) along the cipher text, looking for positions at which there were no matches.

In order to uncover cribs, a 'cribster' often had to read through large quantities of decrypts, keeping meticulous records. As the war progressed, 'cribbing' developed to a fine art. The discovering of cribs presupposes that the message traffic is already being read: the period of work from January 1940 with the perforated sheets and other hand methods was an essential preliminary to the success of the bombe.

In the earlier fictitious example, a mini bomba was used in conjunction with a two-letter crib. One replica of the Simple Enigma was dedicated to the first letter of the crib and another to the second (with the two replicas being set in step at a distance of three, as dictated by the crib). Setting all complications to one side—and in particular *Stecker*—the bombe functions in its bare essentials like the mini bomba in that example.

Suppose we have a message whose first seven letters are

1	2	3	4	5	6	7
B	I	M	Q	E	R	P

and the one-word crib

Z U S T A N D

In a world without *Stecker*, we can exploit the crib by connecting seven replica Enigmas together in such a way that the right-hand wheel (or drum) of the second is one position further on than the right-hand wheel of the first, the right-hand wheel of the third is one position further on than the right-hand wheel of the second, and so on. The seven middle wheels are locked in step in the same position as one another, and likewise the left-hand wheels. As with the set-up procedure for the bomba, this assumes that the middle and left-hand wheels of the sender's machine do not turn over during the first seven letters of the message.

During each run, B is input continuously into the first replica Enigma, I into the second, and so on. The electric motor moves the wheels of each replica Enigma through all their possible positions, one by one. The bombe is set up to stop whenever the letters Z U S T A N D light simultaneously at the seven replica Enigmas. When this happens, the positions of the wheels of the first of the seven are noted. These are candidates for the rod-positions of the wheels at the start of the message.

Each stop is tested by hand, using either a replica Enigma or a British Typex cipher machine set up to emulate an Enigma. (The Typex—also written 'Type X'—was in effect an improved form of the Enigma.[61]) If the rest of the message decodes—or at any rate that part of it up to the point where a turnover of the middle or left wheel occurred—then the correct rod-positions have been found.

The seven replica Enigmas all have the same wheel order. By using more replicas, set up in the same way but with different wheel orders, several wheel orders can be tested simultaneously. Several runs of the bombe are required to test all the possible wheel orders.

If there is no success under the assumption that there were no turn-overs of the middle and left-hand wheels during the enciphering of ZUSTAND, then it is necessary to carry out more runs of the bombe, testing the various possibilities

[61] Bauer, *Decrypted Secrets*, 112, 135.

for when a turnover occurred. Turing describes this procedure in Chapter 6, p. 316.

Once the correct rod-positions are discovered, the wheel order is known and with some trial and error the *Ringstellung* can be worked out. In a steckerless world, the codebreakers now have the daily key and all the intercepted messages encoded on that key can be deciphered. This was done by Typex operators. The messages were decoded by following exactly the same steps that the intended recipient would: the indicator setting, transmitted in clear in the message preamble, was used to decrypt the three-letter indicator, producing the message setting.

Turing's Method for Finding the Plug-Board Settings

Turing employed a simple but brilliant idea in order to deal with the substitutions brought about by the plug-board. He describes this in Chapter 6, which is an extract from his 'Treatise on the Enigma'.[62] (Released in 1996, this material has not previously been published.) 'Treatise on the Enigma' was written in the summer or autumn of 1940 and seems to have been intended for use as a form of training manual.[63] It was known affectionately at Bletchley Park as 'Prof's Book' ('Prof' being Turing's nickname among his colleagues).

Turing's method for finding the plug-board settings dates from 1939. In the example just given, the replica Enigmas are connected 'in parallel'. Turing's idea was to make provision for replica Enigmas (without plug-boards) to be connected nose to tail, with the letter that exits from the wheels of the first being fed into the next in the chain as if it were unsteckered keyboard input. These chains of replica Enigmas could be of varying length, as demanded by the crib.

Each chain exploited a feature of the cribbed message that Turing called a 'closure', but which might equally well be called a 'loop'. There are no closures in the ZUSTAND example. The following, longer, crib (discussed by Turing in Chapter 6, pp. 315ff) contains several examples of closures. (The meaning of the crib is 'No additions to preliminary report'.)

[62] The title 'Treatise on the Enigma' was probably added to Turing's document by a third party outside GC & CS and quite probably in the United States. The copy of the otherwise untitled document held in the US National Archives and Records Administration (document reference RG 457, Historic Cryptographic Collection, Box 201, NR 964) is prefaced by a page typed some years later than the document itself. It is this page that bears the title 'Turing's Treatise on the Enigma'. Another copy of the document held in the British Public Record Office (document reference HW 25/3) carries the title 'Mathematical theory of ENIGMA machine by A M Turing'; this, too, was possibly added at a later date. Mahon refers to the document simply as 'Prof's Book'. The PRO copy is complete, and much more legible than the incomplete NARA copy, which lacks many figures. A digital facsimile of the PRO typescript is available in The Turing Archive for the History of Computing <www.AlanTuring.net/profs_book>. A retyped version of the complete work, prepared by Ralph Erskine, Philip Marks, and Frode Weierud, is available at <http://home.cern.ch/frode/crypto>.

[63] See J. Murray, 'Hut 8 and Naval Enigma, Part I', in Hinsley and Stripp (eds.), *Codebreakers*, 116. The date of composition of the document, summer 1940, is given by Hinsley, *British Intelligence in the Second World War*, vol. iii, part 2, appendix 30, 955.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
D	A	E	D	A	Q	O	Z	S	I	Q	M	M	K	B	I	L	G	M	P	W	H	A	I	V
K	E	I	N	E	Z	U	S	A	E	T	Z	E	Z	U	M	V	O	R	B	E	R	I	Q	T

One closure or loop occurs at positions 2 and 5 and is shown in Figure 9. At position 2, E *encodes* as A and at position 5, A *decodes* as E. Using an upward-pointing arrow to mean 'encodes' and a downward-pointing arrow to mean 'decodes', the loop is as shown in Figure 9.

(Notice that it is equally true that at position 2, A *decodes* as E, and at position 5, E *encodes* as A. It is also true—because the letter substitutions produced by the Enigma are *reversible* (see p. 224)—that at position 2, A encodes as E, and at position 5, E decodes as A. Any of these equivalent ways of describing the loop will do.)

Another closure, this time involving three letters, occurs at positions 5, 10, and 23 (Figure 10). At position 5, E encodes as A, at position 23, A decodes as I, and at position 10, I decodes as E.

E is called the *central* letter of these two closures. The crib contains a number of other closures with central letter E (see Turing's Figure 59 on p. 317).

The point about closures is that they are, as Turing says, 'characteristics of the crib which are independent of the Stecker' (p. 316). Figure 9 tells us that there is

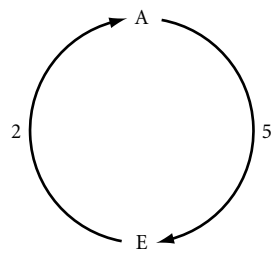

Figure 9. A loop or 'closure'.

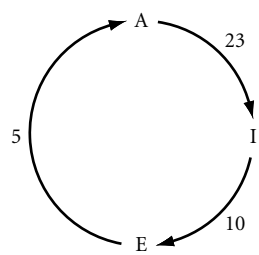

Figure 10. A closure involving three letters.

some letter which, when fed into the wheels at position 2, produces a letter which, if fed into the wheels at position 5, gives the original letter again. At the present stage, we have no idea which letter this is, since unless the central letter E happens to be self-steckered, the letter that goes into the wheels at position 2 is not E itself but whichever letter it is that E is connected to at the plug-board. Turing calls E's mate at the plug-board the 'stecker value' of E. Equally, we have no idea which letter it is that comes out of the wheels at position 2—unless A is self-steckered, the letter that emerges will not be A but A's stecker value.

Figure 10 also represents an assertion about the wheels that is true independently of how the plug-board is set up. There is some letter, *x*, which when fed into the wheels at position 5—that is to say, with the right-hand wheel four clicks further on than at the start of the message—produces some letter, *y*, which when fed into the wheels at position 23, produces some letter, *z*, which when fed into the wheels at position 10, produces *x* again.

As explained below, these closures are used in determining the stecker value of E. Once E's stecker-mate has been found, then the stecker values of the other letters in the loops are easily found out. For example, A's stecker value is whatever letter emerges from the wheels at position 2 when E's stecker-mate is fed in.

Using the Turing Bombe

In Turing's bombe, replica Enigmas without plug-boards are connected into chains that mimic the loops in the crib. In general, a crib containing three or more loops was necessary for Turing's bombe to work successfully.

In the case of the loop in Figure 9, two replica Enigmas are connected nose to tail. The right-hand wheel of the second machine is three clicks further on than the right-hand wheel of the first (because three clicks separate positions 2 and 5). As usual, the wheels are locked in step. To deal with the loop in Figure 10, three replica Enigmas are connected nose to tail. The right-hand wheel of the first machine in the chain is set three clicks ahead of the right-hand wheel of the first machine in the chain that corresponds to Figure 9 (three clicks separating positions 2 and 5). The right-hand wheel of the second machine in the chain of three is eighteen clicks ahead of the right-hand wheel of the first machine in that chain (since eighteen clicks separate positions 5 and 23). The right-hand wheel of the third machine in the chain is five clicks ahead of the right-hand wheel of the first (since five clicks separate positions 5 and 10). Other chains are set up for other closures in the crib also having E as central letter (see Turing's Figure 59 on p. 317).

The bombe works like this. We are going to input the same letter into each of the chains. What we are looking for is the stecker value of the central letter, E. We are going to set about finding it by trying out each of the twenty-six possibilities in turn. First we try the hypothesis that E's stecker-mate is A. So we input A into each of the chains.

The bombe is set up to stop whenever the wheels move into a configuration that produces the input letter—A, during the first run—as the output letter of each of the chains. At any stops during the run, we note not only the positions of the wheels, but also the output letter of each of the replica Enigmas in each chain. If the input letter is indeed E's stecker-mate, and the wheel positions are correct, then these 'interior' letters are the stecker-mates of the intermediate letters of the various closures.

If, in searching through all the possible wheel positions, we find no case in which the last machine in every chain produces A as output, then the hypothesis that E is steckered to A must be incorrect. If, however, we do manage to get A lighting up at the end of every chain, the hypothesis that A is E's stecker-mate remains in the running, and is passed on to someone else to investigate further by hand.

Once the first run is complete, we proceed to the hypothesis that E's stecker-mate is B, and again the wheels are moved through all their positions. And so on, taking each of the twenty-six stecker hypotheses in turn.

Additional runs may be required to test various hypotheses concerning the turnover of the middle and left wheels (as mentioned above). There is also the question of the wheel orders. Typically several different wheel orders will be tested simultaneously. (A thirty-six-Enigma bombe could usually test three wheel orders simultaneously, assuming that no more than twelve Enigmas were required for the loops in the crib.) In the case of an 'all wheel order crib', where no information is available to rule out some of the wheel orders, a number of successive runs, or simultaneous runs on several bombes, will be required in order to examine each possible wheel order.

Unless the data provided by a crib is especially scanty, in which case there might be many stops, this procedure would usually produce a manageably small number of stops. These were tried out manually in another building on a replica Enigma or Typex. Usually the stops were tested more or less as they occurred. As soon as one was found that turned part of the remaining ciphertext into German—albeit German peppered with incorrect letters—the instruction would be telephoned back to the bombe operators to strip the bombe and ready it for the next cribbed message in the queue.

The prototype Turing bombe, named 'Victory', was installed at Bletchley Park on 18 March 1940.[64] It seems to have been used exclusively by Turing and other members of Hut 8 in their attempt to break Naval Enigma.[65]

[64] Hinsley, *British Intelligence in the Second World War*, vol. iii, part 2, appendix 30, 954. When Mahon says in the next chapter that the 'first bombe arrived in April 1940' (p. 292), he is probably referring to the time at which the bombe became available to the codebreakers.

[65] 'Squadron Leader Jones, Section' (Public Record Office, document reference HW 3/164). (Thanks to Ralph Erskine for sending me a copy of this document.)

Simultaneous Scanning

The efficiency of the bombe could be increased greatly by—instead of, as just described, trying out one stecker hypothesis at all positions of the wheels before moving on to the next hypothesis—allowing all the twenty-six possible stecker hypotheses for the central letter (E to A, E to B, etc.) to be tried out together in the short interval before the wheels (drums) shifted from one position to the next. This is 'simultaneous scanning'. Turing's original intention was to include additional electrical apparatus in the prototype bombe to implement simultaneous scanning and he outlines a way of doing this in Chapter 6 (see the section 'Pye simultaneous scanning'—Pye was an electronics company located in Cambridge). However, the problem proved difficult for the engineers and the additional apparatus was not ready in time to be incorporated in Victory.[66] Turing explains in Chapter 6 that the method the engineers were proposing would 'probably have worked if they had had a few more months experimenting', but that their work was in the end overtaken by the discovery of a solution 'which was more along mathematical than along electrical engineering lines' (p. 319).

Turing presents this mathematical solution in two stages in Chapter 6. First he explains (what will in this introduction be called) his *feedback method* (see his section 'The Spider'). This Turing describes as 'a way of getting simultaneous scanning on the Bombe' (p. 323). Then he goes on to explain the role of Welchman's dazzlingly ingenious invention, the *diagonal board* (see Turing's section 'The Spider. A Second Description. Actual Form'). Welchman's diagonal board brought about a dramatic increase in the effectiveness of the bombe.

Turing's Feedback Method

Let us reconsider the previous search for the stecker value of the central letter E. We first tried the hypothesis that E's stecker-mate is A. Inputting A, we rotated the wheels looking for a position at which the letter to emerge is again A. The feedback method is this.[67] Before the wheels are shifted from the current position to the next, whichever letter emerges from the suitably interconnected Enigmas—which will in all probability not be A—is fed back in as the new input letter. (This is done automatically via a braid of twenty-six wires.) This step is then repeated: whichever letter emerges is fed back in, and so on. Unless the first attempt produced A, the effect of these cycles of feedback is that different stecker hypotheses are tested at the current position of the wheels.

If the wheel position is not the starting position for the message then, given a crib with sufficient loops, all twenty-six letters will usually be produced as output during the cycles of feedback. So if the emerging letters are imagined as appearing at a lampboard, all twenty-six lamps will light. At some positions, however—the

[66] Hinsley, *British Intelligence in the Second World War*, vol. iii, part 2, appendix 30, p. 954.

[67] Welchman gives an account of the method, *The Hut Six Story*, 237–41.

interesting positions—not all the lamps light. At these positions it is usually true (again given a crib with sufficient loops) either that only one lamp lights, or that only one remains unlit (a reflection of the fact that the Enigma's letter-substitutions are reversible). Either way, the letter on the odd lamp out is a candidate for the stecker value of the central letter, and the position of the wheels is a candidate for the starting position. Letters produced by other Enigmas within the chains are candidates for the stecker values of other letters of the loops.

The Diagonal Board

Welchman conceived the diagonal board as a way of increasing the effectiveness of the bombe by further exploiting the reciprocal character of the stecker-substitutions. (The substitutions are reciprocal in the sense that if letter L_1 is steckered to L_2 then—owing to the design of the plug-board—L_2 is inevitably steckered to L_1.) With the diagonal board in operation, the bombe could work cribs containing fewer than three closures and even cribs containing no closures at all (as in the ZUSTAND example) provided the length of the crib was sufficient. (If Welchman's diagonal board had never been conceived, bombes of the earlier type could have been used successfully against Enigma networks producing enough cribs with at least three closures—although at the expense of greater amounts of bombe time.[68])

Once Welchman had thought of the diagonal board, Turing quickly saw that it could be used to implement simultaneous scanning. Joan Clarke, who worked alongside Turing in Hut 8, said: 'Turing soon jumped up, saying that Welchman's diagonal board would provide simultaneous scanning.'[69] (Clarke was one of Welchman's mathematics students at Cambridge. For a short period in 1941, she and Turing were engaged to be married.)

The new form of bombe with the diagonal board was initially called the 'Spider' to distinguish it from Turing's earlier form, but soon simply 'bombe' prevailed. (Possibly the name 'Spider' arose in virtue of the practice of using 'web' as a term to refer to the connected parts of a diagram depicting the loops in a crib; see Chapter 6, pp. 325, 329.[70]) The first Spider was installed on 8 August 1940.[71] It was known as 'Agnus', short for 'Agnus Dei' (the name later became corrupted to 'Agnes' and 'Aggie').[72] Agnus contained thirty replica Enigmas, six fewer than in later models. Both Hut 8 (Naval Enigma) and Hut 6 (Army and Air Force Enigma) were given access to the new machine.[73]

[68] C. A. Deavours and L. Kruh, 'The Turing Bombe: Was It Enough?', *Cryptologia*, 14 (1990), 331–49 (346–8).

[69] Murray (née Clarke), 'Hut 8 and Naval Enigma, Part I', 115.

[70] I am indebted to Frank Carter for this suggestion.

[71] Hinsley, *British Intelligence in the Second World War*, vol. iii, part 2, appendix 30, 955.

[72] 'Squadron Leader Jones, Section' (see n. 65); R. Erskine, 'Breaking Air Force and Army Enigma', in Erskine and Smith, *Action this Day*, 56.

[73] 'Squadron Leader Jones, Section'.

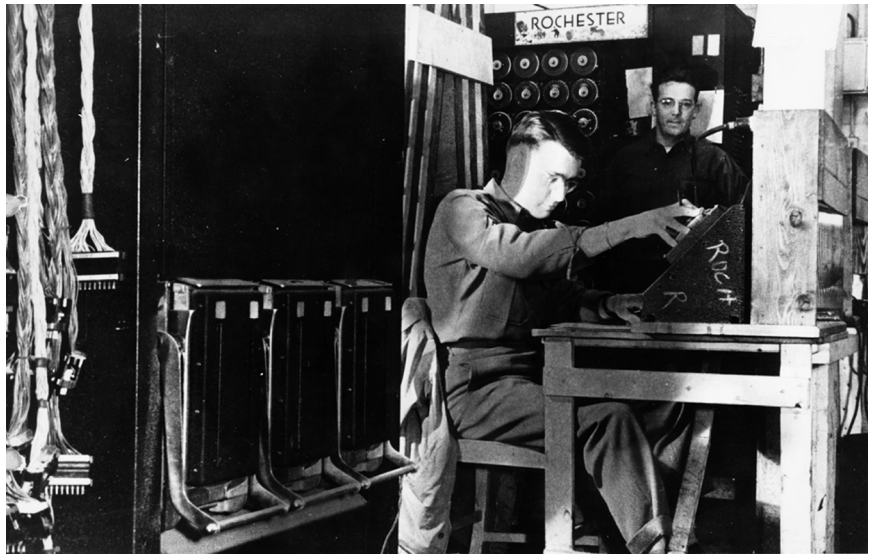

Figure 11. Working in a bombe room at Out Station Eastcote. 'Menus' for the outstation bombes were received from Bletchley Park over a teleprinter line.

Source: Photograph from 'Operations of the 6312th Signal Security Detachment, ETOUSA', 1 October 1944 (NARA, document reference: RG 457, Historic Cryptographic Collection, Box 970, NR 2943).

Subsequent Developments

At first the number of bombes increased relatively slowly, and much of the code-breakers' energy went into the use of hand methods—such as Turing's method of *Banburismus*—designed to reduce the amount of bombe time required to break a crib. By June 1941 there were only five bombes in operation, rising to fifteen by November.[74] The picture changed markedly when a new factory dedicated to the production of bombes came into operation at Letchworth. The output of Enigma decrypts produced by GC & CS more than doubled during 1942 and 1943, rising to some 84,000 per month by the autumn of 1943.[75] Groups of bombes were housed in 'outstations' in the district surrounding Bletchley Park, and then subsequently at three large satellite sites in the suburbs of London, with dedicated teletype and telephone links to Bletchley Park.[76] By the end of the war there were around 200 bombes in continuous operation at these various sites.[77] From August 1943, US Navy bombes began to go into operation in Washington, DC. About 125 were in operation by the time Germany fell.[78] Good cable communications

[74] Alexander 'Cryptographic History of Work on the German Naval Enigma', 31, 35.
[75] Hinsley, *British Intelligence in the Second World War*, ii. 29.
[76] Welchman, *The Hut Six Story*, 139–41, 147.
[77] Ibid. 147.
[78] Erskine, 'Breaking German Naval Enigma on Both Sides of the Atlantic', 192–3.

enabled Bletchley to use the Washington bombes 'almost as conveniently as if they had been at one of our outstations 20 or 30 miles away'.[79]

6. Naval Enigma

Turing's Break

Between 1934 and 1937 the Poles had enjoyed some success against German Naval Enigma. However, on 1 May 1937 a major change of indicator procedure rendered Naval Enigma impenetrable.

During much of 1940 German Air Force traffic was being read in large quantities by GC & CS, but Naval traffic—including the all-important messages to and from the wolf-packs of U-boats in the North Atlantic—remained cloaked. The German strategy was to push Britain toward defeat by sinking the convoys of merchant ships that were Britain's lifeline, bringing food, raw materials, and other supplies across the Atlantic from North America. From the outbreak of war to December 1940 a devastating total of 585 merchant ships were sunk by U-boats, compared to 202 merchant vessels sunk by aircraft during the same period.[80] If Home Waters Naval Enigma (*Heimische Gewässe*)—called 'Dolphin' at Bletchley Park—could be broken, the positions of the wolf-packs in the North Atlantic would be known and convoys could be routed around them.

When Turing took up residence at Bletchley Park in September 1939 no work was being done on Naval Enigma, which some thought unbreakable. As late as the summer of 1940 Denniston declared to Birch, the head of the Naval Section at GC & CS (Hut 4): 'You know, the Germans don't mean you to read their stuff, and I don't suppose you ever will.'[81] This was never the opinion of Birch and Turing. Alexander's history of the attack on Naval Enigma (written at the end of the war and kept secret by the British government until very recently) recounted:

> Birch thought it could be broken because it had to be broken and Turing thought it could be broken because it would be so interesting to break it . . . Turing first got interested in the problem for the typical reason that 'no one else was doing anything about it and I could have it to myself'.[82]

The chief reason why Dolphin was so difficult to break was that the indicator system required the sender to encipher the message setting by two different methods before broadcasting it—once by means of the Enigma machine, as was usual, and once by hand. Mahon describes the procedure in detail in Chapter 5. The hand encipherment was performed by means of a set of *bigram tables*. These tables specified substitutions for pairs of letters, such as 'DS' for

[79] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 90.

[80] S. W. Roskill, *The War at Sea 1939–1945* (London: HMSO, 1954), 615–16.

[81] C. Morris, 'Navy Ultra's Poor Relations', in Hinsley and Stripp (eds.), *Codebreakers*, 237.

[82] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 19–20.

'HG' and 'YO' for 'NB'. Enigma operators were issued with a set of nine complete tables, each table giving substitutions for all the 676 possible bigrams.[83] Which table was to be used on any given day was set out in a calendar issued with the tables. New sets of tables came into force periodically. Crews were under strict instructions to destroy the tables before abandoning ship or if the enemy was about to board.

Turing started his attack exactly where the Poles had left off over two years before, studying 100 or so messages from the period 1–8 May 1937 whose message settings were known. Before the end of 1939 he had fathomed out exactly how the complicated indicator system worked. Chapter 5 contains an extract from Turing's 'Treatise on the Enigma' (published here for the first time) in which Turing explains how he performed this remarkable piece of cryptanalysis.

Hut 8

In 1940 Turing established Hut 8, the section devoted to breaking Naval Enigma. Initially the Naval Enigma group consisted of Turing, Twinn, and 'two girls'.[84] Early in 1940 they were joined by Tony Kendrick, followed by Joan Clarke in June of that year, and then in 1941 by Shaun Wylie, Hugh Alexander, Jack Good, Rolf Noskwith, Patrick Mahon, and others.[85] Turing was 'rightly recognized by all of us as the authority on any theoretical matter connected with the machine', said Alexander (himself later head of Hut 8).[86] In Chapter 5 Mahon recounts how, under Turing's leadership, Hut 8 slowly gained control of Dolphin during 1940 and 1941.

Unlike *Heimische Gewässe* (Dolphin), *Ausserheimische Gewässe*—meaning 'Distant Waters'—would never be broken by Hut 8, and several other Naval Enigma networks also resisted attack.[87] *Süd*, on the other hand, used in the Mediterranean from mid-1941, was a much easier proposition than *Heimische Gewässe*. As Mahon mentions in the next chapter (p. 273), *Süd* employed a version of the indicator system broken by the Poles. *Süd*'s procedure of enciphering the message setting twice (on which the bomby had depended) meant that Hut 8 was able to read *Süd* traffic without any need for cribs.[88]

Pinches

Turing's discovery of how the indicator system worked could not be used to read the German traffic until the bigram tables were known. Materials obtained by the

[83] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 7.

[84] Chapter 5, p. 285.

[85] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 26, 28, 30; Murray, 'Hut 8 and Naval Enigma, Part I', 112.

[86] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 33.

[87] Erskine, 'Breaking German Naval Enigma on Both Sides of the Atlantic', and 'Naval Enigma: The Breaking of Heimisch and Triton', *Intelligence and National Security*, 3 (1988), 162–83.

[88] *Süd* is discussed in Erskine, 'Naval Enigma: An Astonishing Blunder', *Intelligence and National Security*, 11 (1996), 468–73, and 'Breaking German Naval Enigma on Both Sides of the Atlantic', 186–9.

Royal Navy from enemy vessels enabled the codebreakers to reconstruct the all-important tables. (Many of the captures are described in Hugh Sebag-Montefiore's fast-paced book *Enigma: The Battle for the Code*; see the section of further reading.)

The first capture, or 'pinch', of Home Waters daily keys—which Alexander described as 'long awaited'—was on 26 April 1940.[89] A party from the British destroyer HMS *Griffin* boarded an armed German trawler disguised as a Dutch civilian vessel (bearing the false name 'Polares').[90] The trawler was bound for the Norwegian port of Narvik to deliver munitions. The 'Narvik Pinch', as it became known, yielded various documents, including notes containing letter-for-letter cribs for 25 and 26 April (see Mahon's account in the next chapter).[91] Among the documents was a loose scrap of paper (overlooked at first) on which were scribbled the *Stecker* and the indicator setting for 23 and 24 April.[92] Also captured were exact details of the indicator system, confirming Turing's deductions.[93]

The crib for 26 April was tried on the recently arrived Victory, and according to Alexander 'after a series of misadventures and a fortnight's work the machine triumphantly produced the answer' (see also p. 286, below).[94] Alexander reports that 27 April could then also be broken, the 26th and 27th being 'paired days'—days with the same wheel order and *Ringstellung*.[95] Thanks to the Narvik Pinch, the days 22–5 April were also broken (not on the bombe but by hand methods).[96]

Another pinch was needed if Dolphin was to be broken for any substantial period. Various plans were discussed. One, code-named 'Operation Ruthless', was masterminded by Lieutenant Commander Ian Fleming of Naval Intelligence, who later created the character James Bond. Mahon describes the plan, which he credits to Birch, in the next chapter. In the event, Operation Ruthless was not carried out. Turing's reaction is described in a letter by Birch dated 20 October 1940:

[89] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 24.

[90] The report of the engagement, 'Second and Last War Cruise', is in PRO (document reference ADM 186/805). See also R. Erskine, 'The First Naval Enigma Decrypts of World War II', *Cryptologia*, 21 (1997), 42–6.

[91] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 24; Ralph Erskine (personal communication).

[92] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 24; Murray, 'Hut 8 and Naval Enigma, Part I', 113.

[93] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 24.

[94] Ibid. 25.

[95] Ibid. 5, 25.

[96] Alexander's statements on pp. 24–5 (or possibly Mahon's on p. 286, below) have been interpreted, probably incorrectly, by the authors of *British Intelligence in the Second World War* as implying that materials obtained from the Narvik Pinch enabled Hut 8 to read Naval Enigma traffic for the six days 22–7 April *during May* (Hinsley et al., *British Intelligence in the Second World War*, i. 163, 336). In 1993 Joan Clarke stated that some of these days were not broken until June (Murray, 'Hut 8 and Naval Enigma, Part I', 113; see also Erskine, 'The First Naval Enigma Decrypts of World War II', 43).

Turing and Twinn came to me like undertakers cheated of a nice corpse two days ago, all in a stew about the cancellation of operation Ruthless. The burden of their song was the importance of a pinch. Did the authorities realise that . . . there was very little hope, if any, of their deciphering current, or even approximately current, enigma for months and months and months—if ever? Contrariwise, if they got a pinch . . . they could be pretty sure, after an initial delay, of keeping going from day to day from then on . . . because the level of traffic now is so much higher and because the machinery has been so much improved.[97]

Turing did not get what he wanted until the 'Lofoten Pinch' of March 1941, which Mahon describes as 'one of the landmarks in the history of the Section' (p. 290). On 4 March, during a commando raid on the Norwegian coast—planned with a pinch in mind—the Royal Navy destroyer HMS *Somali* opened fire on the German armed trawler *Krebs* near the Lofoten Islands.[98] *Krebs* was boarded and tables giving the daily keys for the complete month of February 1941 were captured.[99] Short of obtaining the bigram tables as well, this was exactly what was needed. A month's daily keys were sufficient to enable Hut 8 to reconstruct the tables.[100] Suddenly Hut 8 was properly open for business and by the beginning of April was looking forward to breaking the Naval traffic 'as nearly currently as possible'.[101]

Eager to follow up on the *Krebs* success, Harry Hinsley in Hut 4 put forward a plan to capture a German weather ship, *München*, operating north-east of Iceland.[102] On 7 May 1941 *München* was duly boarded by a party from the *Somali*.[103] The booty included the daily keys for the month of June. The July keys soon followed, captured from the weather ship *Lauenburg* in another raid planned by Hinsley.[104] The capture of the June and July keys helped Hut 8 reconstruct the new bigram tables issued on 15 June (see the next chapter).[105] The new tables were current until November 1941.[106]

During June and July Hut 8 was producing decrypts of Enigma messages within one hour of their being received. Mahon says on pp. 290–291, 'There can be no doubt that at this stage the battle was won and the problem was simply

[97] Birch's letter is included in a contemporary report entitled 'Operation Ruthless' by C. Morgan (PRO document reference ADM 223/463).

[98] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 27. An official report of the operation is in PRO (document reference DEFE 2/142). The operation is described in Erskine 'Breaking German Naval Enigma on Both Sides of the Atlantic', 178.

[99] Chapter 5, p. 290; Alexander, 'Cryptographic History of Work on the German Naval Enigma', 27.

[100] Chapter 5, p. 290.

[101] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 28.

[102] Hinsley, *British Intelligence in the Second World War*, i. 337.

[103] A report of the capture is in PRO (document reference ADM 199/447).

[104] Hinsley, *British Intelligence in the Second World War*, i. 337.

[105] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 31.

[106] Ibid. 7.

one of perfecting methods, of gaining experience, and of obtaining and above all of training staff.'

Probably the most dramatic pinch of all occurred to the south of Iceland on 9 May 1941, during the pursuit of the submarine *U-110* by several Royal Naval vessels acting as convoy escorts.[107] Sub-Lieutenant David Balme, of the destroyer HMS *Bulldog*, led the party that boarded the stricken submarine. In an interview Balme described the depth-charging of the *U-110*:

> Suddenly two ships were torpedoed one after the other. It was obvious where the attack had come from and the corvette *Aubretia* made a very accurate attack on the U-boat. Must have got the depth-charges just at the right depth. It was a classic attack: depth-charges underneath the U-boat blew it to the surface. It was the dream of every escort vessel to see a U-boat blown to the surface. Usually they just sink when you have a successful attack.

The German crew abandoned ship shortly before Balme boarded the U-boat. He continued:

> I couldn't imagine that the Germans would have abandoned this U-boat floating in the Atlantic without someone down below trying to sink her. But at any rate I got on and got my revolver out. Secondary lighting, dim blue lighting, was on and I couldn't see anybody, just a nasty hissing noise that I didn't like the sound of.[108]

But the U-boat was deserted and, inexplicably, the Germans had made no attempt to destroy the Enigma materials on board. Balme and his men carried off the Enigma machine and the bigram tables. However, the tables had already been reconstructed laboriously by Turing and co. (see p. 290). Balme's pinch was not of major significance to Hut 8 and does not even rate a mention by Mahon or Alexander.

Banburismus

Another of Turing's pivotal contributions to the breaking of Naval Enigma was his invention of the hand method called *Banburismus*. The name arose because the method involved the use of specially made sheets bearing the alphabet which, being printed in the nearby town of Banbury, came to be called 'Banburies'. Mahon records that Turing invented the method the same night in 1939 that he worked out the indicator system (see Chapter 5).

The aim of Banburismus was to identify the day's right-hand and middle wheels. This meant that fewer wheel orders had to be tried on the bombe, thereby saving large amounts of bombe time. During the years when so few bombes were available, it was Banburismus which made it possible to read Dolphin. As Mahon

[107] The official account of the pursuit is in PRO (document reference ADM 1/11133). See also R. Erskine, 'Naval Enigma: A Missing Link', *International Journal of Intelligence and Counterintelligence*, 3 (1989), 493–508.

[108] Balme interviewed on British Channel 4 TV, 1998.

says, for two or three years Banburismus was 'the fundamental process which Hut 8 performed' (p. 281). Banburismus was discontinued in September 1943, bombes being plentiful enough by that stage.

The Battle of the Atlantic

Hut 8's ability to decode the U-boat messages had an immediate effect on the course of the war.

At the beginning of June 1941 Churchill had been informed by his planners that, as a result of the attacks on convoys, Britain's predicted imports amounted to substantially less than the minimum quantity of food necessary to keep the population fed during the remainder of 1941.[109] Oil and other imports would also arrive in insufficient quantities for war production to be maintained. The U-boats were crippling Britain. However, during June 1941—when Dolphin was read currently for the first time—reroutings based on Hut 8 decrypts were so successful that for the first twenty-three days of the month, the North Atlantic U-boats made not a single sighting of a convoy.[110]

The pattern continued in subsequent months. The Admiralty's Operational Intelligence Centre (OIC) became increasingly skilled at evasive routing based on Bletchley's Ultra intelligence, and the wolf-packs spent more and more time searching fruitlessly.[111] Although Hut 8's battle with the U-boats was to see-saw—for eleven long months of 1942, Hut 8 was blacked out of the North Atlantic U-boat traffic by the new fourth wheel inside the Enigma—the intelligence from Naval Enigma decrypts played a crucial role in the struggle for supremacy in the North Atlantic.

7. Turing Leaves Enigma

Mahon records that towards the end of 1941 Turing was running out of theoretical problems to solve concerning Naval Enigma (p. 312). Soon Turing was taking little part in Hut 8's activities. His talent for groundbreaking work was needed elsewhere.

For a period during 1942 Turing rejoined the Research Section to work on the new problem of 'Tunny'.[112] From June 1941 GC & CS had begun to receive enciphered messages that were very different from the Enigma traffic. These were carried by an experimental radio link between Berlin and Greece. Numerous other links soon came into existence, connecting Berlin to German Army Group commands throughout Europe. Unlike Enigma radio transmissions, which were

[109] Hinsley, *British Intelligence in the Second World War*, ii. 168–71.

[110] Ibid. 171.

[111] Ibid. 169–70, 172–5.

[112] W. Tutte, 'Bletchley Park Days', in B. J. Copeland (ed.), *Colossus: The First Electronic Computer* (Oxford: Oxford University Press, 2005).

in Morse code, the messages on these links were broadcast in binary teleprinter code. The British code-named the machine encrypting the new traffic 'Tunny'. Tunny was one of three different types of non-Morse 'Fish' traffic known to Bletchley (the others were codenamed 'Sturgeon' and 'Thrasher').

It was not until July 1942 that up-to-date Tunny traffic was read for the first time, by means of a paper-and-pencil method invented by Turing and known simply as 'Turingery'.[113] The Germans used Tunny for high-level Army communications and sometimes messages signed by Hitler himself would be deciphered.[114] With the arrival of the 'Heath Robinson' in June 1943, followed a few months later by the first of the electronic Colossus computers, the Tunny traffic, like Enigma before it, succumbed to the Bletchley machines (see further the introductions to Chapters 4 and 9).

Alexander gradually took over the running of Hut 8. In November 1942, Turing departed for the United States, where he liased with the US Navy's codebreakers and bombe-builders.[115] He was never to do any more work in Hut 8.[116] Following his return to Bletchley, in March 1943, he held a wider brief, acting as scientific policy adviser.[117] Turing eventually left Bletchley Park at the end of 1943, moving to Hanslope Park to work on the problem of automatically enciphering speech. He remained at Hanslope until the end of the war.[118]

In his history of Bletchley's attack on Naval Enigma, Alexander included the following appreciation of Turing's 'great contribution':

> There should be no question in anyone's mind that Turing's work was the biggest factor in Hut 8's success. In the early days he was the only cryptographer who thought the problem worth tackling and not only was he primarily responsible for the main theoretical work within the Hut (particularly the developing of a satisfactory scoring technique for dealing with Banburismus) but he also shared with Welchman and Keen the chief credit for the invention of the Bombe. It is always difficult to say that anyone is absolutely indispensable but if anyone was indispensable to Hut 8 it was Turing. The pioneer work always tends to be forgotten when experience and routine later make everything seem easy and many of us in Hut 8 felt that the magnitude of Turing's contribution was never fully realized by the outside world.[119]

[113] I. J. Good, D. Michie, and G. Timms, 'General Report on Tunny' (1945), 458. 'General Report on Tunny' was released by the British government in 2000 to the Public Record Office (document reference HW 25/4, HW 25/5). A digital facsimile is in The Turing Archive for the History of Computing <www.AlanTuring.net/tunny_report>.

[114] Peter Hilton in interview with Copeland (July 2001).

[115] S. Turing, *Alan M. Turing* (Cambridge: Heffer, 1959), 71. Turing's report 'Visit to National Cash Register Corporation of Dayton, Ohio' (n.d.; *c.* Dec. 1942) is now declassified (document reference: NARA, RG 38, CNSG Library, 5750/441). A digital facsimile of the report is in The Turing Archive for the History of Computing <www.AlanTuring.net/turing_ncr>.

[116] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 42.

[117] S. Turing, *Alan M. Turing*, 72; Don Horwood in interview with Copeland (Oct. 2001).

[118] There is an account of Turing's Hanslope period on pp. 269–90 of Hodges's biography (see the section of further reading in 'Alan Turing 1912–1954', above).

[119] Alexander, 'Cryptographic History of Work on the German Naval Enigma', 42–3.

In July 1941 Turing, Alexander, and Welchman were summoned to the Foreign Office in London to be thanked for what they had done.[120] Each was given £200 (a sizeable sum in those days—Turing's Fellowship at King's paid him less than twice this amount per annum). At the end of the war, Turing received the Order of the British Empire for the role he had played in defeating Hitler—a role that, after more than half a century of secrecy, has only now come fully into the light of day.[121]

Further reading

Bauer, F. L., *Decrypted Secrets: Methods and Maxims of Cryptology* (Berlin: Springer-Verlag, 2nd edn. 2000).

Budiansky, S., *Battle of Wits: The Complete Story of Codebreaking in World War II* (New York: Free Press, 2000).

Erskine, R., and Smith, M. (eds.), *Action This Day* (London: Bantam, 2001).

Hinsley, F. H., and Stripp, A. (eds), *Codebreakers: The Inside Story of Bletchley Park* (Oxford: Oxford University Press, 1993).

Kahn, D., *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939–1943* (Boston: Houghton Mifflin, 1991).

Sebag-Montefiore, H., *Enigma: The Battle for the Code* (London: Weidenfeld and Nicolson, 2000).

Smith, M., *Station X: The Codebreakers of Bletchley Park* (London: Channel 4 Books, 1998).

Welchman, G., *The Hut Six Story: Breaking the Enigma Codes* (Cleobury Mortimer: M&M Baldwin, 2nd edn. 2000).

[120] Diary of Sir Alexander Cadogan, Permanent Under-Secretary at the Foreign Office, 15 July 1941: Andrew, *Codebreaking and Signals Intelligence*, 3.

[121] I am grateful to Friedrich Bauer, Frank Carter, Ralph Erskine, John Harper, Diane Proudfoot, and Frode Weierud for their comments on a draft of this chapter.