Alan Turing: Life and Legacy of a Great Thinker

Bearbeitet von
Christof Teuscher, D Hofstadter

1st ed. 2003. 2nd printing 2005. Buch. xxviii, 542 S. Hardcover
ISBN 978 3 540 20020 8
Format (B x L): 15,5 x 23,5 cm
Gewicht: 1116 g

Weitere Fachgebiete > EDV, Informatik > EDV, Informatik: Allgemeines, Moderne Kommunikation > EDV & Informatik: Geschichte

Zu Inhaltsverzeichnis

Alan Turing at Bletchley Park in World War II

Tony Sale

Ex Museums Director, Bletchley Park, UK

Summary. "There should be no question in anyone's mind that Turing's work was the biggest factor in Hut 8's success [in breaking the German Naval Enigma]. 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" [1].

1 Alan Turing and the Enigma Machine

The mathematician Alan Turing had been identified, at Cambridge, as a likely candidate for code breaking. He came to the Government Code and Cypher School (GC&CS) in Broadway in London a number of times in early 1938 to be shown what had already been achieved. He was shown some intercepts of German signals enciphered on the German forces Enigma cipher machine.

The Enigma machine, Fig. 1, was an electro/mechanical way of achieving a seven, or nine, layer substitution cipher. The individual substitutions were fixed by wiring within wheels which could be rotated by the operator but which also index round, like a car miles indicator, as letters to be enciphered or deciphered were entered.

The Enigma was patented in 1918 by Arthur Scherbius in Berlin, developed by him as a commercial product and shown to the public in 1922.

Because the machine could be bought by anyone, the security of the cipher depended not on the machine itself but on the vast number of ways in which it could be configured before the start of an encipherment.

To increase the complexity of this setting up, each wheel had a tyre, or ring, round the core containing the cross wiring. Letters or numbers on the surface of this ring appeared in the windows above each wheel. The ring could be rotated around the core and set by the operator before encipherment began. It remained set throughout the message input.

The action of pressing a key caused the right hand wheel to index one position (one of 26). At some point this rotation was transferred to the next wheel on the left. This was known as a carry and was caused by a slot,

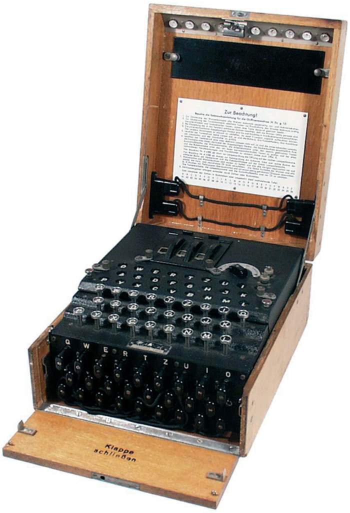

Fig. 1. A German Army/Airforce Enigma Machine

the carry slot, coming into line with the indexing pawls. This carry slot was initially on the wheels; later it was moved to the ring.

An electrical current was used to sense the substitutions. When a key was pressed a connection was made from the battery to a point on the fixed entry disc on the right hand side of the wheels, AFTER the right hand wheel had indexed and any carry had caused other wheels to turn ... The electrical current flowed through the internal wiring in the wheels from right to left, was turned round in the reflector and came back through the wheels to exit at a different point on the entry disc which was connected to a lamp on the lamp panel. The lamp that lit was the encipherment of the key just pressed.

The clockwise order of connections to the fixed, right hand, entry disc was known as the "entry order." In the Scherbius commercial machine this was just the order of the keys on the keyboard from left to right across each of the three rows. This was known as the `QWERTZUIO` order.

Thus the variable elements of the Enigma were: the wheels and their order from left to right in the machine, the ring setting for each wheel, the wheel rotational position, the start position before encipherment started.

The first Enigma machines, the glow lamp machines of the 1920s, had three wheels which could be removed and replaced in any order. (6 combinations). The reflector was rotatable by the operator (26 positions). The wheel start positions thus gave 26 × 26 × 26 positions. The ring settings gave a 26 position rotational translation of each wheel start position. Total number of different configurations, $2,741,856$.

From 1930 the plug board (Stecker) was added to the Enigma used by the German Army and Air Force. The plug board enabled pairs of letters to be completely transposed. Initially 6 pairs were transposed, later this was increased to 10, the nearly optimum number. At the same time the reflector became fixed. This machine was then also adopted by the German Navy.

For this Enigma the wheels give $6 \times 26 \times 26 \times 26 = 105,456$ possible combinations. Six plug pairs gives $100,391,791,500$ possibilities; total approximately ten thousand, million, million (10^{17}).

Despite this seeming invulnerability due to such a vast number of possible configurations, the Enigma machine had some weaknesses. Firstly because of the reflector no letter could encipher to itself. Secondly, each of the first set of wheels, 1 to 5, had a different point at which turnover occurred to the next wheel on the left. This allowed identification of the right hand wheel and sometimes even the centre wheel. (The later Naval Enigma wheels 6, 7 & 8 had two carries, all at the same wheel positions.)

In London, in 1938, Alan Turing would have met Alistair Denniston, the head of GC&CS and Edward Travis, Hugh Foss, John Tiltman and Dilly Knox, all eminent code breakers, some from World War I.

Edward Travis had purchased a commercial Enigma machine in 1925 and Hugh Foss had devised a geometric way for breaking it in 1927. Later, in 1936, Dilly Knox devised his "rods" method for breaking the unsteckered Enigma used in the Spanish civil war which also had the `QWERTZUIO` entry order and the same rotor wiring as the commercial Enigma.

Meanwhile in Poland the Polish Security Service had purchased a commercial Enigma and worked out, in the 1920s, methods for breaking it. When, in 1930, the Germans changed to the steckered Enigma, the Poles recruited some young mathematicians to try to break it. The greatest of these was Marian Rejewski who found ways of exploiting the German procedural mistakes in using Enigma. The problem for the Germans was how to tell the intended recipient of an enciphered message the exact wheel start letters from which the message could be deciphered. They decided to encipher this start position, known as the message key, on the Enigma machine itself in order to conceal it from any interceptor. But they also enciphered it twice in order to make certain that it was correctly received by the intended operator.

It was this double encipherment which Marian Rejewski exploited in his very successful "characteristics" method of attack. He also correctly deduced that the Germans had changed the entry order to `ABCDEFG` ... and worked out the new wheel wirings which were different from those in the commercial machine. Later he devised a machine called a "Bomba" specifically to attack the double encipherment of the message key.

In 1938 Dilly Knox already knew that the German forces Enigma rotors were wired differently to the commercial rotors, but did not know the entry rotor order and apparently did not know of the double encipherment of the message key.

All the Polish achievements were divulged to the British and the French at the famous meeting in the Pyry Forest near Warsaw in July 1939.

In September 1939 Turing came to Bletchley Park and joined Dilly Knox in the cottage in the stable yard. He started to think of ways to break Enigma using probable words, "cribs" and was intrigued by the problems in breaking the German Naval Enigma.

The method based on probable words was a far more powerful method than that used in Rejewski's Bomba and led later to the development of the Turing Bombe.

GC&CS already had a few intercepts and at least one plain text/cipher text pair, reputed to have been smuggled to England by a Polish cipher clerk.

2 "Cribs" and Opened Out Enigmas

2.1 Letter Pairs

Among the characteristics that Turing found in these messages was that occasionally the same cipher/plain text pair of characters occurred at different places in the same message.

```
JYCQRPWYDEMCJMRSR
SPRUCHNUMMERXEINS
```

Remember that because the Enigma machine is reversible, R→C is the same as C→R and M→E the same as E→M.

Whether such pairings occur is determined by the rotor order and the core rotor start positions. Turing realized that conversely the actual rotor order and core rotor start position could be arrived at by trying all configurations to see if these pairings were satisfied and more importantly he realized that this was independent of the Steckers.

Obviously just setting up a single Enigma machine and trying by keying in would take an impossibly long time. The next step was to consider how the tests could be carried out simultaneously for a particular Enigma start configuration. Testing for letter pairs required a method for rapidly determining whether such a configuration was true or false. This led to the concept of electrically connecting together a number of Enigma machines (Fig. 2).

This was achieved by using an "opened out" Enigma (Fig. 3). In the actual Enigma electrical current enters and leaves by the fixed entry rotor because of the reflector or Umkerwaltze (U) and this precluded connecting Enigmas together. In Turing's opened out Enigma the reflector had two sides, the exit side being connected to three rotors representing the reverse current paths through the actual Enigma rotors. This gave separate input and output connections and thus allowed a number of Enigmas to be connected in series.

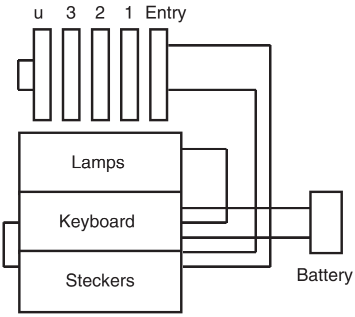

Fig. 2. Enigma schematic

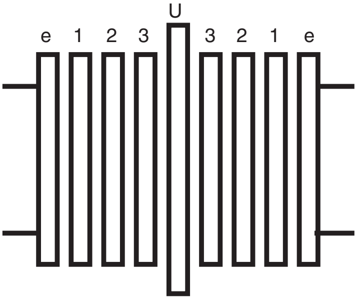

Fig. 3. Opened out Enigma

In the Letchworth implementation (Fig. 4), the clever thing was to include both forward and backward wiring of an Enigma rotor in one drum. The connections from one drum to the next were by four concentric circles of 26 fixed contacts and four concentric sets of wire brushes on the drum. Three sets of fixed contacts were permanently wired together and to the 26 way input and output connectors. Three drums, representing the original Enigma rotors, could now be placed on shafts over the contacts and this was an opened out Enigma with separate input and output connectors.

To return to the problem of checking whether C enciphers to R (written as C→R), first an offset reference from the start is required. A lower case alphabet written over the cipher text gives this.

```
abcdefghijklmnopq
JYCQRPWYDEMCJMRSR
SPRUCHNUMMERXEINS
```

This shows that C→R at offset c, e and l from the start (see Fig. 5), and M→E at j, k and n. The opened out Enigma allows an electric voltage to be applied to the input connection “C” and a set of 26 lamps to be connected

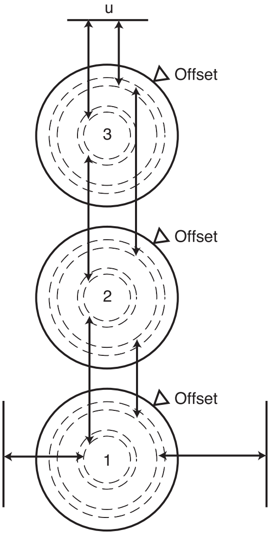

Fig. 4. Letchworth Enigma

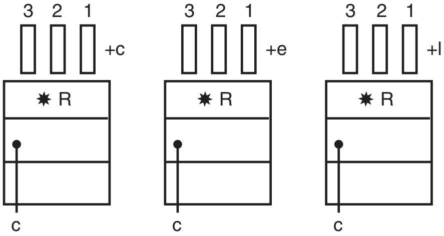

Fig. 5. Separate Enigmas testing for CR

to the output connector. If the R lamp lights then the drums are in an order and position such that C enciphers to R.

With a single Enigma this can occur at a vast number of drum settings. However the crib allows an opened out Enigma to be set up for each occurrence of C→R (Fig. 6) and they can then all be tested simultaneously.

The opened out Enigmas are all set up with the same drum order and the drums are then turned to the same settings for the left hand and middle drums but the right hand drums are turned to the offset letter along the crib at which the test is to be made. All the inputs are connected in parallel and a voltage applied to the "C" contact. Then a set of relays connected to each of the "R" output contacts tests to see if all the R contacts have a voltage on at the same time. When they do a position of the drums has been found which satisfies the crib at the points chosen for C→R (Fig. 6).

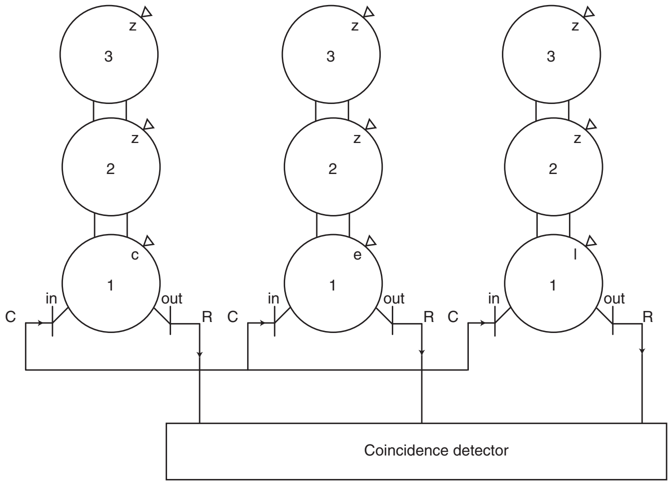

Fig. 6. Letchworth Enigmas testing for CR

If they don't then all the right hand drums are advanced one position and the test is tried again. After 26 positions of the right hand drum the centre drum is advanced one position and this continues until all drum positions have been tested. Then the drums are changed to try a different drum order. A very long process by hand which obviously asks to be automated.

This can be achieved by an electric motor driving all the right hand drums simultaneously and then "carrying" to the middle drum every 26 positions, with a further carry from the middle to left hand rotor when this has turned through 26 positions. In this way the drums can be driven through all 17,576 possible positions and the occurrence of a correct position for all C→R in the crib can be checked.

But there are still a large number of positions which satisfy the C→R test. What is needed is a better method for finding the rotor order and rotor setting.

2.2 Letter Loops and Steckers

An extension of the concept of letter pairs is where letters enciphered from one to another at different places in the crib resulting in loops of letters.

```
abcdefghijklmnopq
JYCQRPRYDEMCJMRSR
SPRUCHNUMMERXEINS
```

For instance R→N at g, N→S at p and S→R at q making a loop (Fig. 7). A diagram showing such loops was known as a menu (Fig. 8).

But if Steckers are being used this is actually:

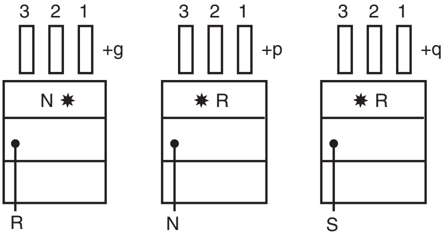

Fig. 7. Separate Enigmas Testing for RNS

- R steckered to S1 enciphers to S2 steckered to N at g
- N steckered to S2 enciphers to S3 steckered to S at p
- S steckered to S3 enciphers to S1 steckered to R at q (see Fig. 9).

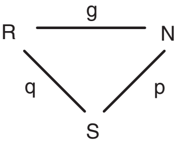

Fig. 8. A menu

The problem now is to find the core positions S1, S2 and S3. If these can be found then they are the Steckers of the menu letters.

But Turing realized that there was another way of looking at interconnected opened out Enigmas and that this way found Stecker connections.

Take the loop example above of R→N→S→R. Three opened out Enigmas are connected serially one to the other and the right hand drums are turned to the offsets g, p and q. If the correct drum order is being used then there will be some start position of the left had, middle and right hand drums which corresponds to the actual original Enigma core rotor positions having allowed for the difference between the original Ringstellung and ZZZ. At this point the core rotor positions will be the same as the original Enigma core rotor positions and the encipherments will then be the same.

This means that a voltage placed onto the S1 input of the first opened out Enigma, which is the Stecker of the input R, will come out on the S2 terminal which is the Stecker of N. Since this is connected to the next opened out Enigma, this goes in on its S2 terminal and comes out on the S3 terminal which is the Stecker of S. This S3 input now goes through the third opened out Enigma and comes out at S1 which is the Stecker of R. Thus the drum positions correspond to the original Enigma positions where S1→S2→S3→S1.

The magic trick is now to connect the output terminals of the last opened out Enigma back to the input of the first Enigma. There is now a physical wired connection through the opened out Enigmas from the S1 input terminal to the S1 output terminal which is now connected to the S1 input terminal. This forms a loop of wire not connected to any other terminals on any opened out Enigma (Fig. 10).

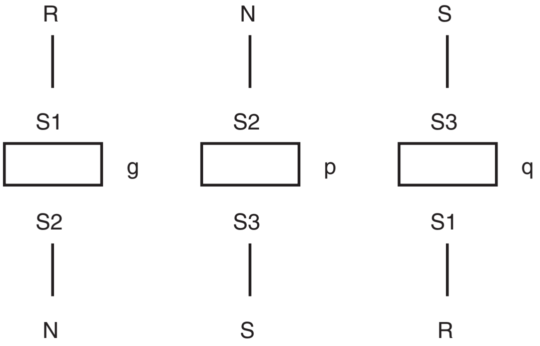

Fig. 9. Including Steckers

Thus if a voltage is placed on S1 at the input it goes nowhere else, just appears on the S1, S2 and S3 terminals. If a strip of 26 lamps is connected at the joins between opened out Enigmas then the S1, S2 and S3 lamps will light confirming the voltage path through S1, S2 and S3.

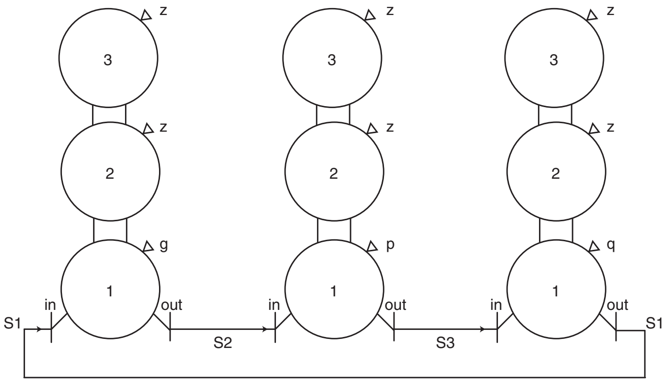

Fig. 10. Letchworth Enigmas connected as a menu

Now comes Turing's really clever bit. If S1 is not known and the voltage is placed on, say, A then this voltage will propagate through the opened out Enigmas because they are joined around from output to input, but *cannot* reach the S1, S2, S3 loop because it is not connected to any other terminals. The voltage runs around the wires inside the opened out Enigmas until it reaches a terminal which already has the voltage on it. The complete vastly complex electrical network has then reached a steady state.

Now if the lamp strip is connected at the joins of the opened out Enigmas, lots of lamps will light showing where the voltage has reached various terminals, but the appropriate S1, S2 and S3 lamps will not light. In favourable circumstances 25 of the lamps will light. The unlit lamp reveals the core letters, S1, S2 or S3. These are interpreted as the Steckers of the letters on the menu.

When the drum order and drum positions are correct compared to that of the original core Enigma encipherment there is just the one wired connection through the opened out Enigmas, at connections S1, S2 and S3. But Turing also realised that such a system of joined opened out Enigmas could rapidly reject positions of the drums which were not the correct ones.

If the drums are not in the correct position then the loop S1, S2, S3 does not exists and the voltage can propagate to these terminals as well. Thus it is possible for the voltage to reach all 26 terminals at the join of two of the opened out Enigmas. This implies that there is no possible Stecker letter and therefore this position of the drums cannot be correct. But because of the way the cross wiring inside real Enigma rotors is organised, closed loops of connections can occur which are not the loops corresponding to the actual Stecker connections being looked for. The configuration of opened out Enigmas cannot distinguish between these spurious loops and the correct Stecker loop.

The test for a loop of possible Steckers at a particular drum order and rotor position is to see if either only one or 25 of the lamps are lit. If all 26 lamps light then this position can be rejected and this rejection can occur at very high speed. The voltage flows around the wires at nearly the speed of light so that the whole complex network stabilises in fractions of a microsecond. What was required was some way of automating the changes of drum position for all the drums in synchronism and for rapidly sensing any reject situation.

In 1939 the only technology available for achieving electrical connections from rapidly changing drum positions was to use small wire brushes on the drums to make contact with fixed contacts on the Test Plate. This was a proven technology from punched card equipment. High speed relays were initially the only reliable devices for sensing the voltages on the interconnections. Thermionic valves were tried but were not reliable enough in 1939. Later, thyratron gas filled valves were used successfully and these were about 100 times faster than the high speed relays.

The British Tabulating Machine Co (BTM) had designed the opened out Enigmas and built the Test Plate. The project to now build a complete search engine, which became known as a Bombe, came under the direction of H. H. (Doc) Keen.

The machine, known as Victory, was completed by March 1940 and delivered to Bletchley Park. It was first installed in one end of Hut 1. Now the work began on finding out how to use this new device. Results at first were not very encouraging. The difficulties in finding cribs meant that when a menu was constructed between intercepted enciphered text and a crib, it usually did not have enough loops to provide good rejection and therefore a large number of incorrect stops resulted.

3 The “E” Rack

In November 1939, Alan Turing proposed a letter frequency attack using what he called the “E” rack (see also Sect. A). There are no surviving documents giving any details of what was proposed but a modern computer simulation, Virtual E rack, shows that it would have been feasible.

3.1 Letter Frequency

The basis of this attack is that the frequency of occurrence of some letters of natural language is very far from random. For instance, in German and English the letter E occurs at about 12% compared with a random score of 4%. Code breakers had long ago realised this, it was used to attack Caesar’s substitution ciphers. What Alan Turing realised was that it could be mechanised along similar lines to his development of the Turing Bombe.

If a length of cipher text could be deciphered simultaneously by lots of Letchworth Enigmas and the number of output E counted, then a correct setting would show as a large count of E, but more importantly an incorrect setting could be rapidly rejected by a low count of E.

3.2 Minimum Length of Cipher Text

The first question is how long must the cipher text be to obtain a significant result. Measurements on some original deciphered German messages showed an E frequency of one in eight letters. (Oliver Lawn’s 1941 paper gives one in 8.34 over 5,410 German message letters). This agrees with the 12% quoted elsewhere.

However, what is more important for the determination of minimum length is the maximum distance between E in messages. Examining archive German decrypts gives 8 for the average but a long tail out to 34 as the maximum inter E distance in these messages.

Successive starting point lengths of 50 letters gives a minimum of 2 Es for an average of 4. 80 letter lengths give minimum 5 and length 120 gives minimum 9.

Next question; what are the maximum counts of any letter when a length of cipher text is deciphered on the wrong Enigma setting. The Virtual E rack enables this to be measured by setting the cut off limit so low that all decipherments are shown. One result is that for a cipher length of 70, E max on the correct settings is 9 but E count off the correct settings also can be 9 as are the maximum counts for non E off the correct setting. However, a cipher length of 130 letters gives a count of 25 on E max correct with counts of 17 for E on incorrect and for other letters' maxima.

So it would appear that a cipher length of over 100 letters is required to get a clear indication of the correct setting and this is confirmed by Virtual E rack.

3.3 Limitations on the Use of the E Rack

Most importantly the Steckers (plug board connections) must be known or mostly all known. The reason for this is that a letter substitution on the output side would just mean a different letter giving a maximum in place of E if E was steckered. But missing or wrong substitutions on the input side completely change the encipherment.

Virtual E rack will work with one Stecker pair missing and sometimes with two, but it depends which two.

Then there is wheel turnover. Because the ring settings are not known (ZZZ is assumed), any turnover in the course of encipherment of the original message is not reproduced. Virtual E rack tries to take care of turnover in the right hand to centre wheels by deciphering the cipher text consecutively at two turnover points on the right hand wheel; 2 and 16 are used. This means that the decipherment will only be wrong for a maximum of half a wheel rotation for one of the two settings. (I tried using 3 decipherments at about 8 position intervals but the improvement was so slight it was thought better to go faster on two).

3.4 So Where Could the E Rack Be Used?

Firstly Turing et al in their original November 1939 note suggested it could be used against German Naval Enigma. The problem, at that time, was the lack of complete Bigram tables. Some entries had been worked out by Turing, but only very few. This meant that although they could sometimes find the settings for one message, they could not decipher other messages because they couldn't decode the message keys, the wheel start positions.

But if they had found the Steckers from the message they had broken, then the E rack could be used to find the wheel starts for the other messages.

However the capture of the complete Bigram tables probably rendered the E rack unnecessary.

4 Adding the Diagonal Board to the Bombe

Soon after the first Bombe came to Bletchley Park, Gordon Welchman came up with the idea of the diagonal board. This was an implementation of the simple fact that if B is steckered to G then G is also steckered to B. If 26 rows of 26 way connectors are stacked up, then any connection point can be referenced by its row letter and column letter. A physical piece of wire can now connect row B element G to row G element B. The device was called a Diagonal Board because such a piece of wire is diagonally across the matrix of connections.

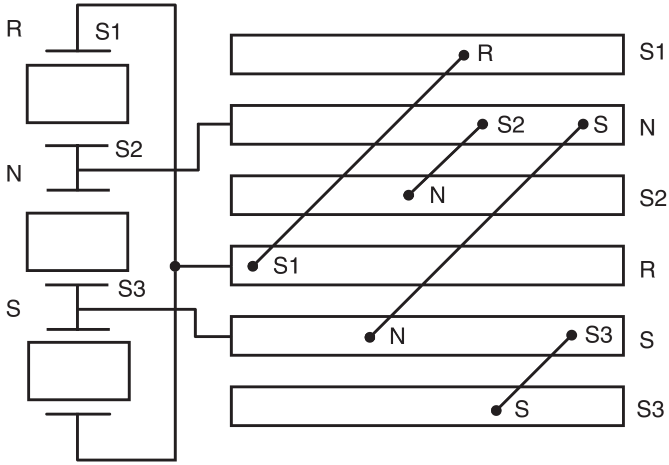

Fig. 11. The Diagonal Board

Now the double ended Enigma configuration knows nothing about Steckers. It can only deduce rotor core wiring positions which satisfy the menu. However the possible Steckers such as R↔S1, can by exploited by the Diagonal Board. If the joins between double ended Enigmas are also connected into the Diagonal Board at the position corresponding to the original cipher/plain text pair on the menu, say R, then this can significantly increase the rejection of incorrect double ended Enigma drum positions.

It has already been shown that if a set of drum positions has been found where S1→S2→S3→S1 then a physical wired connection has been made through the joins between opened out Enigmas at S1, S2 & S3. The deduction from this is that R is steckered to S1, etc. Now if the join representing R on the menu is plugged to the R row of the Diagonal Board, a physical piece of wire will connect through the Diagonal Board from row R at position S1 to row S1 at position R. Since S1 is not plugged to anything the voltage on this wire goes nowhere else. Similarly for the other joining positions between opened out Enigmas. Thus the Diagonal Board does not affect the finding of the correct drum positions.

But if the drums are not in the correct position to make the connection S1, S2 & S3, then a voltage travelling around the network and finally arriving at say row N position S will be passed via the Diagonal Board wire to row S position N and will thus continue through the wiring in the opened out Enigmas on both sides of the join S. The Diagonal Board thus greatly contributes to the voltage flow around the network of wires in the opened out Enigmas due to the extra connectivity that it provides. This increases the rejection of drum positions which do not satisfy the menu.

5 Alan Turing and the German Navy's Use of Enigma

5.1 Why Naval Enigma was Difficult

At first sight it is not obvious why Naval Enigma was so difficult; it initially used the same version of Enigma as the German Army and Air Force and these were broken virtually throughout the War. The difficulty lay in the indicator system. This was unique to the German Navy and involved a separate coding system, bigrams and trigrams, for concealing the message setting. As will be explained, it was this indicator system which made the breaking of Naval Enigma so difficult and it had defeated the Poles.

Alan Turing started where the Poles left off, with the 100 or so messages from May 1st–8th 1937 whose starting positions were known.

From these he had the two four letter groups, the indicators, from each message and also the message setting, i.e., the start position for deciphering the message which the Poles had found.

Using these and some very elegant deductions, Turing worked out the complete indicator system.

At the same time, as he later said, "I thought of the method of Banbarismus, but was not sure that it would work in practice." This was at the end of 1939.

A summary document on the Naval Enigma Situation (see Sect. A) was produced in November 1939, signed by Dilly Knox., Peter Twinn, Gordon Welchman, Alan Turing and John Jeffreys. It was Appendix II in the original document. It proposes a "rack" as a method for solving Enigma. I don't think that this was ever built. It was overtaken by Turing's work on his Bombe.

In early 1940, joined by Peter Twinn, Turing started an attack on messages for 28th November 1938 using FortyWeepyWeepy cribs. The reason for going back so far was that only 6 Steckers were being used at that time and the FortyWeepyWeepy cribs were working. These were broken after a fortnight's work and four other days also came out.

The name FortyWeepyWeepy arose from the German habit of starting a continuation part of a message (Fort in German) with the time of origin of the first part using the top row of the keyboard as numbers, $Q = 1$, $W = 2$ etc. with Y as a figure shift showing that the following letters should be interpreted as numbers. Hence continuation part of a message originated at 23.30 hrs started with `FORT Y WEEP Y WEEP Y`.

There was also a paper method which involving representing the Enigma wheels by strips of paper or card. Turing called these "comic strips." A colour coding was used to identify the Enigma wheels.

These breaks were helped by the first use of the EINS catalogue.

5.2 The EINS Catalogue

Once messages began to be deciphered, it was realized that the German word EINS was by far the most frequent word in Naval messages.

It was then decided to take on the prodigious task of cataloguing the encipherment of EINS at all $105,000$ possible start positions (on the three wheel Enigma). This was done *by hand*.

Later it was put onto punched cards for Freeborne's section, the large punched card processing section, to use.

To use the EINS catalogue consecutive groups of four letters in the message were looked up to see whether they were an encipherment of EINS.

Then with an Enigma machine set to these settings the characters following what was thought to be EINS were deciphered to see if German came out.

5.3 The Code Breaker's Problem

The first difficulty was working out the Bigram Tables. This had to start with a "pinch," i.e., a capture of a set of tables. Once message breaking had started, it was possible, with some difficulty, to work out new bigram tables. The tables were changed roughly once a year.

In order to decipher all the messages intercepted on a given day it was necessary to recover all of the daily key, i.e., Wheel Order and Wheel Start for deciphering the message key (the Grund) and the Steckers.

There are 336 WO's and $26 \times 26 \times 26$ start positions, i.e., about $6,000,000$ combinations to examine to find the right one. This requires a test to distinguish between a right and a wrong position and a very rapid means of applying this test.

5.4 Naval Enigma “Cribs”

A Crib in BP terminology was a guess at a section of the German text that was enciphered to give the intercepted enciphered message. Such a guess required clues and the Germans provided these in abundance.

- Because of the length, time of origin, call sign, etc., of a message it probably began with a phrase like

  `VORHERSAGEBEREICH SIEBEN` (weather forecast for area seven).
- Routine messages were sent out day after day at about the same time, from the same place, of the same length and starting in exactly the same way
- Re-encodements. These were retransmissions of messages already sent on some other key

Cribs allowed the deduction of menus for running on the Bombes. But initially there were very few Bombes and running 336 wheel orders just consumed too much time. This is where Banburismus came in. It significantly reduced the number of wheel orders to be run, sometimes to only 20.

5.5 Banburismus

Banburismus could be used if there were two lengths of cipher text and from the trigrams it was thought that they may have been enciphered from nearly the same wheel start positions. Banburismus enables the finding of the difference in start positions of the two texts. This only works because the letter distribution of language text is not flat random.

In Fig. 12 you can see the definitely non random spread of text letters and the much more nearly random cipher text spread.

Because some text letters occur much more frequently than others, there is a strong possibility that in two displaced texts there will be coincidences of these letters. When these two texts are enciphered on an Enigma machine, these points of coincidence of the letters will result in the same enciphered letters. Thus by looking for cipher text displacements at which there are more than random coincidences of cipher letters, the difference in start of encipherment can be deduced.

Banbury Sheets, so called because they were printed in Banbury, a town about 30 miles away from Bletchley, enabled the relative start positions of two cipher texts to be discovered.

These sheets had up to 200 alphabets running side by side vertically down the sheet with A at the top.

The girl in the Big Room in Hut 8 first went along the Banbury Sheet marking each letter of the cipher text with a red marker, then she took the sheet to a punch machine and punched a round hole through each marked letter.

```
    H
    H
    H                  H
    H                  H
    H                  H
    H                  H
    H         H  H     H
    H        HH  HH    H
H H H  HH H  HH  HHH  HH
HHHHHHHHH HH HH  HHH  HH
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Text 1

```
          H     H
H HHH H   H   H H H   H
HHHHHHH   HH HH H H   HH H
HHHHHHHHHHHHHHHHH HHH HH H
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Cipher 1

Fig. 12. Letter histograms

Then by sliding sheets one above the other and counting the letter coincidences, it was possible to determine the offset at which the two messages had been enciphered.

The importance of this was that no turnover could occur within this distance and by accumulating information from a number of cipher text pairs, it was possible to eliminate wheels which could not be in the right hand position.

It was usually possible to be certain of the right hand wheel number, and most times to get the middle wheel as well.

This would reduce the number of wheel orders to be run from 336 down to possibly 20.

If a good crib was available this could be run on the Bombes, otherwise a special menu could be built up based on the trigram distances.

5.6 The "Narvik Pinch"

A trawler intercepted on April 26th 1940 by the destroyer *Arrow* proved to be a disguised German ship. A boarding party recovered one of two bags thrown overboard by the crew. It contained the Stecker and Grundstellung for April 23rd and 24th and an operator's log giving letter for letter cribs for April 25th and 26th.

The bag also contained exact details of the indicating system which confirmed Turing's deductions and the E tables used for short rapid communications and a description of how they worked; The "Long E bars" (Alfa-Funksignale) was a system for rapid communication by ships in action, it was a good source of cribs.

5.7 Early Banburismus

The Doldrums — May '40 to February '41. Following the Narvik Pinch, giving Stecker and Grund, April 23rd and 24th were easily broken and "paired days" i.e., the same WO and Ringstellung, soon followed.

April 26th proved difficult. Hand methods failed because of 10 Stecker pairs. However the first Bombe had just arrived and a crib from the operator's log was tried. After a series of misadventures and a fortnight's work, the Bombe triumphantly produced the answer.

With the 26th out, the paired day, the 27th, was soon broken and both days were found to be on the same bigram table. Every effort was then made to break all the messages on those days in order to recover as much as possible of the bigram table. Banburismus could then be tried on days using this table. But Banburismus proved to be very difficult in practice. May the 8th, the most promising day, was worked on ad nauseam for months.

Foss's Day. In August, Mr Foss returned from sick leave, was given May 8th and by sheer perseverance broke it in November. May 8th is immortalized as Foss's Day.

The reasons for this long period of the doldrums were: incomplete bigram tables, lack of cribs and a large number of "Dummy" messages.

August 25th 1940, Frank Birch wrote to Travis saying:

> I'm worried about Naval Enigma. Turing and Twinn are like people waiting for a miracle, without believing in miracles ...

Then came the Lofoten raid and the Enigma keys for February 1941 from the Krebs.

5.8 The Heydays of Banburismus

April 1941–February 1942. The capture of the February '41 keys allowed the bigram tables to be built up completely. All April and May except 6th May were broken, but not currently.

The capture of the June keys covered the change in bigram tables on June 15th. With increased staff, although the first six days of August proved difficult, Banburismus was now so refined that September 18th/19th were the only days not broken on DOLPHIN for the rest of the war.

Banburismus was now breaking a few hours after the completion of a day's traffic and if the next day was a "paired day," breaking could be current.

These Pinches were absolutely essential, there were just too many unknowns in Naval Enigma for it to be worked out cryptographically.

The Doldrums Again — February to August 1942. On February 1st 1942 SHARK went onto an entirely separate key using 4 wheels instead of 3 and a new reflector. This was the M4, the German Navy's four wheel Enigma.

5.9 The 4 Wheel Enigma

The M4 used the same mechanical structure as the Naval three wheel Enigma but fitted a rotatable fourth wheel and a thin reflector in the space occupied by the reflector in a three wheel Enigma. It used:

1. Two fourth wheels, Beta and Gamma
2. Two "thin" reflectors, Bruno and Ceasar
3. Any combination could be used
4. A combination stayed in force for one month
5. Beta and Gamma ring setting always at Z
6. The fourth wheel could be set to any of 26 positions but did not turn during message entry
7. With the fourth wheel set to A, and a matching reflector, the machine was equivalent to a three wheel Enigma
8. The number of start positions was now $26 \times 26 \times 26 \times 26 = 456,976$

The wiring of wheel and reflector had been given away by German security blunders. An operator failed to set the fourth wheel in neutral, "A," and put it at "B" instead. Thus

```
Time 14.47 date 17/12/41  From W/T Station Adm.
Comm. U-Boats. E bar 551, Service No 166 wrongly
enciphered. Contents: U.131 reports: Am able to
dive. Have been hunted by 4 destroyers.

Time 16.30 date 17/12/41. From Mueller. E bar
551 deciphers with setting B.
```

Another good source of cribs was a reencipherment from DOLPHIN of Admiral Doenitz's message to the Fleet on succeeding Admiral Raeder.

Although there had been some advanced warning of the coming of the 4 wheel Enigma, the first design of a four wheel Bombe was not very satisfactory. This was the Wynn-Williams design of a high speed fourth wheel attachment to the three wheel Bombe. It was connected to the Bombe with a very long thick cable and was known as "Cobra."

The Americans were by now suffering from U Boat raids on their East Coast so they decided to build their own four wheel Bombes. Alan Turing went to America on 7th November 1942 to liase with the Americans on their four wheel Bombe design.

Doc Keene, at BTM, produced a four wheel version of the three wheel Bombe. This worked fine but was not as fast as the American four wheeler. By the time the fourth rotor came fully into service, high speed 4 wheel Bombes had been developed, which together with the weather cribs got back into Shark with the help of the American 4 wheel Bombes.

6 Alan Turing after German Naval Enigma

6.1 Lorenz

In summer 1942 Turing became involved with the breaking of the Lorenz teleprinter cipher system. Bill Tutte had worked out the original structure of Lorenz and Turing devised a statistical method for helping to get out wheel patterns, known as "Turingismus." This was superseded when the Colossi became available.

6.2 Alan Turing Leaves Bletchley Park

By late 1943 his work on code breaking in Bletchley Park was all but complete and he moved to nearby Hanslope Park to work on his ideas for a speech enciphering system he called "Delilah."

Together with Don Bayley he started constructing Delilah in June 1944. It was finished on VE Day, 6th May 1945.

7 An Appreciation of Alan Turing at Bletchley Park

Hugh Alexander wrote in his History of Naval Enigma [1]:

> 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 realised by the outside world.

A Appendix II of UK Public Record Office Document HW14/2

APPENDIX II

NAVAL ENIGMA SITUATION

The solution of Naval Enigma will divide itself into two parts, that of solving one message of a day, and that of solving further messages.

The first problem is to be tackled by:

(a). Analytical methods, using Jeffrey's statistics (virtually hopeless).

(b). By the machine now being made at Letchworth, resembling, but far larger than the Bombe of the Poles (superbombe machine).

If one message is solved by one of these means we shall have the machine settings for the day, viz: Walzenlage, Steckerverbindungen, Ringstellung, but not Grundstellung nor list of bigrams used in the indicating system. We might also obtain the Stecker by capture.

For the second problem; i.e. solving further messages, we may either:

(i) Guess three or four letters of the message.

(ii) Make use of another machine, the "rack", which operates by so setting the messages that the decode contains sufficiently many letters E.

We have at present no information which will be of use for Method (i), although when a number of messages have been solved it may be applicable. Without a "rack" we shall, therefore, not be able to get any further if, for instance, position Stecker were captured from a submarine.

With the "rack" we shall, in such cases, almost certainly be able to solve 40% of the messages, and probably 70%. If by that time we are able to apply Method (i) as well, we may be able to solve as many as 200 messages on that day. If this ever happens it will be possible to solve the indicating system; i.e. to obtain the bigram list. This will enable us to solve all further messages for that day at once, and, on later days while the bigram list lasts, to solve all messages as soon as a single message has been solved for that day.

We feel that no unnecessary time should be lost in experimenting with and constructing such a machine.

SIGNED: A.D. KNOX
P.F.G. TWINN
W.G. WELCHMAN
A.M. TURING
J.R. JEFFREYS
1st November. 1939.

(UK Public Record Office online catalogue: http://catalogue.pro.gov.uk.)

References

1. C. H. O'D. Alexander, *Cryptographic History of Work on the German Naval Enigma*. Public Records Office, Kew, Surrey, HW 25/1.