MAPLE VALLEY HAMLINK

VOL. 16 May 2009 Special Edition

THE CODE BREAKERS AT BLETCHLEY PARK

by Richard, KR7L

[*Editors Note*: By request, the series of articles on the World War II code breakers at Bletchley Park is reproduced in this special issue of the *Hamlink*. Additional text and photos are included.]

One of our most interesting places to visit on our journey last fall was the historic site of **Bletchley Park**, home of Britain's now famous but previously best kept secret World War II code breakers known as the National Codes Centre. Situated in a beautiful parkland setting, with a lake, wildlife and an American Garden Trail 50 miles northwest of London, Bletchley Park was previously the home of wealthy financier Sir Herbert Samuel Leon from 1882 to 1926. During the Second World War it was acquired by the British government to house the Government Code and Cypher School. Commanded by Alastair Denniston, the Park and was given the cover name Station X, being the tenth of a large number of sites acquired by *MI6* for its wartime operations.

Photos by the author

"The Mansion" at Bletchley Park

The use of secret codes or ciphers by the military to prevent the enemy from intercepting and gaining knowledge about their operations has been common over the years. In 1915 two Dutch Naval Officers, Spengler and von Hengel invented the first cipher machine that incorporated moving rotors. The Dutch Navy decided not to adopt this machine, but a Dutch businessman, Hugo Koch, took out a patent for a similar machine in 1919. In 1922 Koch shared his patent with a German company, Scherbius & Ritter, who began to manufacture their first cipher machine in 1923. A director of the company, Dr. Arthur Scherbius, who was responsible for the engineering development of the machine, named it the "**Enigma**"

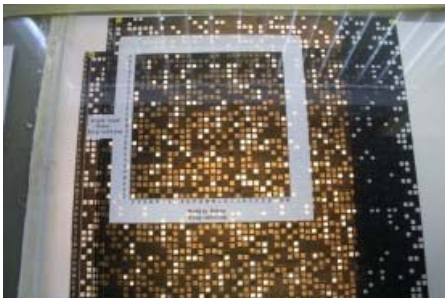
The Enigma

It was initially designed to secure banking communications, but achieved little success in that sphere. The German military, however, were quick to see its potential. They thought the ciphers to be unbreakable, and not without good reason. Enigma's complexity was bewildering. Typing in a letter of plain German into the machine sent electrical impulses through a series of rotating wheels, electrical contacts and wires to produce the enciphered letter, which lit up on a panel above the keyboard. By typing the resulting code into his own machine, the recipient saw the deciphered message light up letter by letter. The rotors and wires of the machine could be configured in many, many different ways. The odds against anyone who did not know the settings being able to break Enigma were a staggering 150 million million million to one.

The Enigma's three wheels

The Polish Intelligence Service began to study the German Enigma

(Continued from page 1)
ciphers in 1926 but had little success. Much later they recruited three young mathematicians, Marian **Rejewski**, Henry **Zygalski**, and Jerzy **Rozycki**, to work in the General Staff's Cipher Bureau. Using an adapted ciphering machine of the commercial type and a "day's keys" supplied by the French intelligence, Rozycki, together with Zygalski, for the first time read secret German messages dating from



The Zygalski Sheets

September through October 1932. Zygalski later developed "perforated sheets", which when laid out on a light table, allowed Enigma messages to be read through a process of trial and error. The explanation of how it was done is rather lengthy but extremely interesting if you wish to pursue it.

Amateurs Recruited for Secret Work

Ham radio operators played a major roll in the secret wireless intelligence war between 1939 and 1945, by providing Bletchley Park with vital messages that enabled the code breakers to read German signals. They were known as Voluntary Interceptor or "VIs" and around 1,200 were recruited by the **Radio Security Service** (RSS). Some of them had powers to enter premises where they thought illicit wireless activity was going on. When World War II began, all radio amateurs had to hand in their transmitters but were able to keep their receivers, subsequently used by the RSS to listen in to enemy wireless traffic in their own homes or even the garden shed.

At its peak the RSS had an organization of 2,094, comprising 98 officers, 1,317 operators, 83 engineers and 471 administrative personnel and 125 civilian clerks, plus the 1,200 amateur radio Voluntary Interceptors. During the war 268,000 RSS decrypts were issued by Bletchley Park, with a peak of 282 a day in May 1944. Of these 97,00 were in Abwehr (German Intelligence) hand cipher and 140,000 enciphered on the Enigma machine.

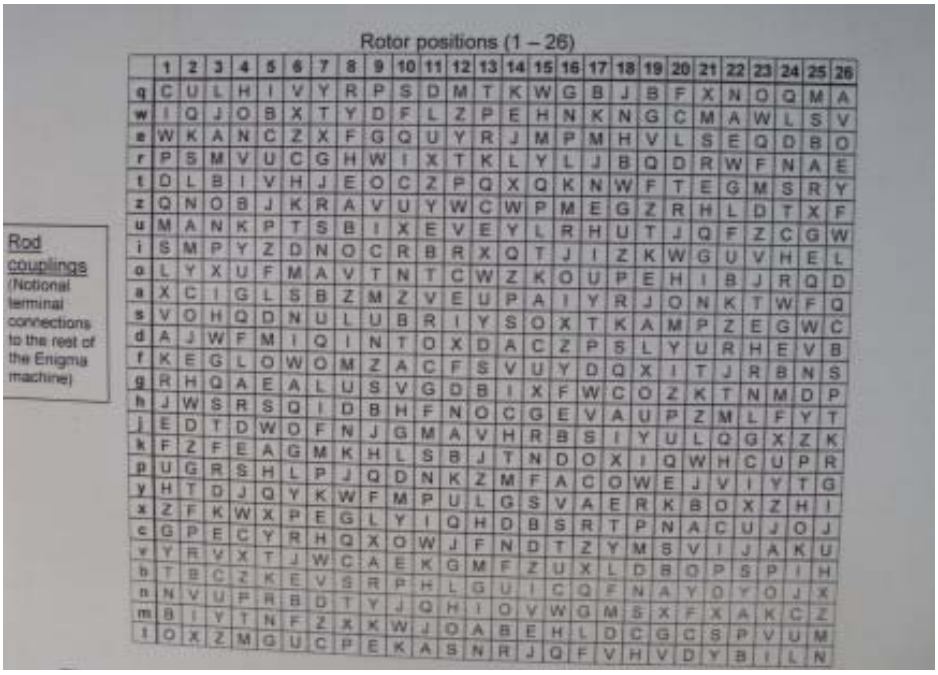
(Continued on page 3)

An example of the listening equipment used by the Radio Security Service Voluntary Interceptors

A Memorial Honoring the Polish Mathematicians

Deciphering of the Enigma messages

In 1937 a distinguished cryptographer **Dilly Knox** developed a method for breaking ciphers that were produced on the early "non-plugboard" versions of the Enigma machine. This technique became known as "Rodding". For each Enigma rotor it was possible to construct a table known as its "rod square". An example of a rod square is shown below:-



The square can be cut horizontally into twenty-six individual strips, and these form the set of rods for the given rotor. For example here is a rod obtained from the first row of the square:-

The invention of the rods provided a method of breaking the Italian Enigma ciphers for which only modest physical resources were needed. However the technique was a demanding one for the cryptographers involved, requiring considerable linguistic skills and a high level of perseverance. In fact there were only a few very talented people who could use the rods effectively.

It was necessary to have three sets of rods available, one set for each of the rotors being used in the Italian Enigmas machine. These rotors had colors designated to them for the purpose of identification, and so did the rods, the three sets being colored red, green and blue.

Meticulous care was required to identify the correct set of rods to use for a particular cipher message, and also their initial starting position. Success then depended upon linguistic ability and creative imagination, so that the nature of the work was not unlike the solving of a difficult crossword puzzle in a foreign language.

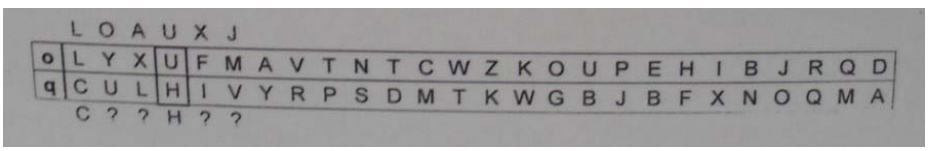
An Enigma machine was set up with the rotor for the given rod square in the right-hand location, initially set to its 1st position. For example if the word "**CIPHER**" were enciphered on the Enigma machine the resulting sequence of letters might be "**LOAUXJ**". The objective was to show the recovery from the enciphered text of a *second* letter of the original plain-text, using its first letter C as a "crib".

Two particular rods were selected from the set for the rotor, the first rod was selected because it has the letter L at its first position, likewise the second rod was selected because it has the letter C at its first position.

The two rods are aligned underneath the sequence of cipher letters (as shown on the next page), with the pair of letters L and C on the rods vertically below the letter L at the 1st position in the cipher. It should be apparent that each letter in this pair is the enciphered form of the other. **This relationship applies to <u>all</u> the pairs of letters formed by the two rods at the other successive positions on the rods.** For example, at the 2nd position on the rods Y is the enciphered form of U and vice-versa, but as neither of these two letters occur in the cipher at this position, the relationship is of no practical use. However at the 4th position the rods provide the pair of letters U and H, and at this position the letter U also occurs in the cipher sequence. Consequently it can be *inferred* that the fourth letter in the original word is H.

So beginning with a short crib, the rods enabled a few other isolated letters from the plain text to be identified, and it was necessary for the code breaker to make inferences for some of the whole words in a message from this fragmented evidence. The rods could then be used to check on the accuracy of

A short "crib" guess

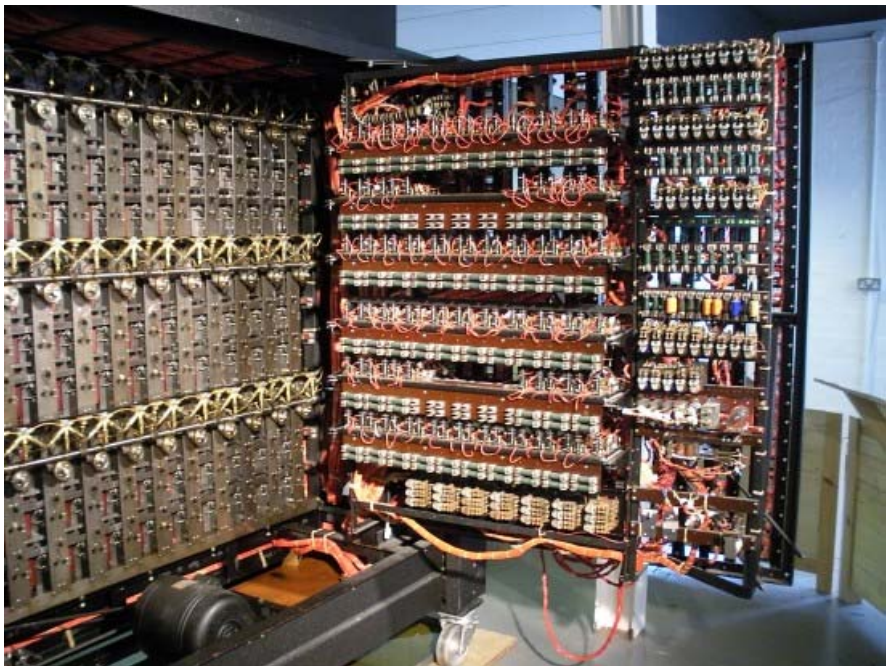


these words, which if correct, could then be used to extend the decryption process further. A more detailed explanation cannot be given here.

If your first inspired guess of the crib was wrong, you had to start over.

It was crucial to the World War II effort to be able to decode the Axis Powers secret military messages quickly. The slow laborious process of using the Zygalski perforated sheets and Dilly Knox's rods could not allow timely usage of the intelligence so gained. So a mechanized process was imperative to speed up the decoding.

A machine was developed to aid the code-breaking method being used by Alan Turing and colleagues at Bletchley Park. The general concept came from Turing and was improved by Gordon Welchman. This machine was named the "**Bombe**". The Bombe was probably named by the Poles who invented the *precursor* to the Bombe shown here. The story goes that they wanted a code name for their machine and were eating a particular type of ice cream called a "bomba" at a café, so used this name. When the British built their machine the name became corrupted to "Bombe" and it stuck.



The Bombe back view

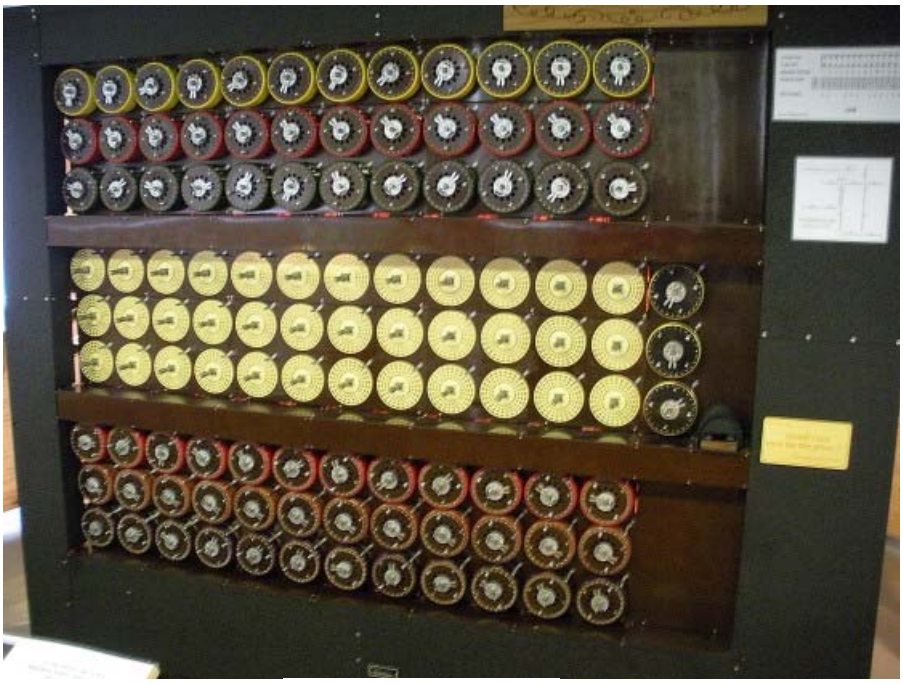
When the first machine worked successfully in 1941, it used the most advanced electro-mechanical technology available.

By the end of the war there were about 200 Bombe machines working but not very many at Bletchley Park. Most were at outstations such as Eastcote and Stanmore.

They were well-maintained and worked around the clock. At the end of the war all the Bombe machines were supposedly broken up and destroyed. However, there are some reports that suggest one of each type was preserved and walled up at Eastcote. These may later have been moved to Cheltenham.

Historians believe that the activities at Bletchley Park shortened the war by as much as two years. Without the Bombes little of this would have been possible

(Continued on page 5)



The Bombe front view

Part 3—How the Bombe was used to break Enigma Ciphers

To decipher the Enigma messages transmitted by the Germans during World War II, it was necessary to determine the "key" that had been used to encipher them. The key was changed at least once each day and was chosen from about 158 million, million, million possible choices.

The Bombes were used to find the following three important parts of a key from a selected message:

1. The identity of the three rotors that had been used, and the positions in which they had been located in the Enigma machine (this was known as the "**rotor order**").
2. Some of the pairs of letters that had originally been chosen for the plug-board cross-connections. It was standard German practice to select a total of ten pairs, and at Bletchley Park they were known as the "**steckers**" (the German word for a plug).
3. The **starting positions** of the rotors for the given message.

If the key for the selected message was found, than all other messages transmitted over the same link on the same day could be easily deciphered. To make use of the Bombe it was necessary to presume a short sequence of the plain-text occurring in the selected message, and to match the letters in it with the corresponding ones from the cipher. This task was called finding a "**crib**" (a short sequence of plain-text together with the corresponding sequence of cipher-text letter that had been obtained from an unbroken message by means of an *informed guess*), and success depended on having experience of the likely content of some of the intercepted signals together with a good knowledge of the German language. Many of the routing Enigma enciphered messages were heavily stereotyped, so clues, such as the message call signs, time of transmission and the length of message often enabled parts of the cipher-text to be correctly inferred.

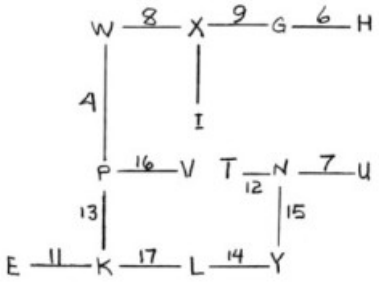
Here an example is shown based on a German Air Force signal (dated November 1, 1944) from the Bletchley Park Trust Archives. The original Bletchley Park decrypt of the message is also available and part of this has been used to construct an example of a crib

Position	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
Cipher	V	S	I	W	M	H	N	X	G	M	K	N	K	L	N	V	K
Plain-text	A	M	X	P	O	G	U	W	X	B	E	T	P	Y	Y	P	L

The "crib"

Some of the pairs of letters in this crib have been used to construct a diagram known as a **menu**:

You can follow this menu starting at the upper right by seeing that



A ""menu"

in the crib in position 6 the letter H in the cipher is paired with the letter G in the plain text. Next in crib position 9 the letter G is paired with the plain-text letter X, and so forth.

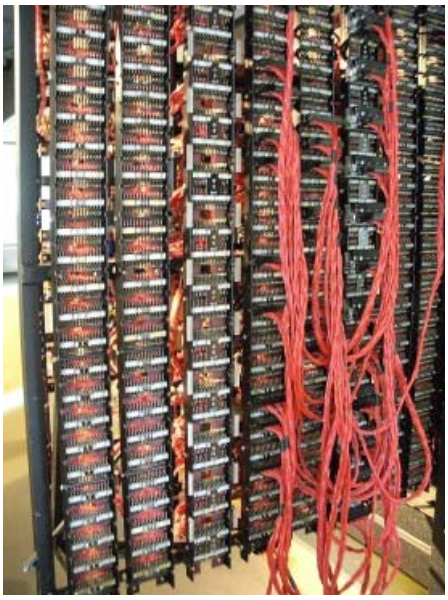
A menu like this was used as the basis for an electrical circuit that was "plugged up" on the back of the Bombe with "steckers", shown in the photo to the right.

Each possible rotor order would then be tested in turn in the following way:

The corresponding set of removable rotor drums was placed on the Bombe and turned to the relative positions given by the numbers on the menu. (In reality, the drums had letter scales marked on them, and these letter scales were used instead of the numbers as are shown on the above menu.)

While the general concepts of the Bombe were provided by Bletchley Park, it fell to the **British Tabulating Machine Company** (similar to IBM) design team at Letchworth in north Hertfordshire to design a practical machine. The first machine was built from scratch in nine months. However, this was not quite the best solution and a modified version arrived six months later and was immediately successful.

The Bombe "steckers"



The Bombes were mostly operated by WRNS (Women's Royal Navy). They set up the machines to the menu and loaded it into the machines by plugging up the cables on the rear of the Bombe. This was very physical work and took about 30 minutes to set up the machine.

There would be maintenance teams who looked after the machines. They were usually civilians in RAF uniform, plus, unusually, one of the WRNS. The gentlemen were either of a technical background, typically GPO (General Post Office) trained, or men with a history of being able to keep a secret.

When in operation, the drums on the Bombe rotated systematically in step through all of the possible starting positions, and at each the machine carried out an electrical test to determine if each letter in the crib was correctly enciphered as the corresponding letter in the cipher message. If the conditions of the test were satisfied then the Bombe would stop. Each stop provided a rotor order and a set of starting positions, together with one "stecker" pair. Collectively they formed part of a possible Enigma key.

After the Bombe operators had recorded this information, the "run" would be resumed, and the information obtained from the "stop" was subjected to further tests and rejected if it was found to be "false" (determined by certain logical considerations). This work was carried out on a small hand operated device known as a "**Checking machine**". On the Checking Machine an entry key was pressed to match the first letter in the menu, and a lamp would light to indicate the exit letter for this part of the menu. This exit letter key was then pressed and so on, until the whole menu had been worked on and the resulting letter matched the first one. This indicated a valid "stop". If the letter did not match then this was not a valid "stop".

If all of the "stops" obtained were shown to be "false" then another trial would have to be made using a different rotor order. When there was no prior knowledge about the correct rotor order, up to sixty Bombe runs might have been necessary. Only one "stop" would provide the Enigma key.

The "false stops" were due to the effects of random chance, and the number obtained depended on the characteristics of the menu. The correct "stop" that would ultimately lead to the complete Enigma key could only be identified by eliminating the "false" ones.

The code breaker's dilemma was that the information shown on the above menu was based on the *assumption* that during the original encipherment of the message a *middle* rotor "turn-over" had not occurred within the "span" of the crib. If this was not the case, then the menu would be invalid and all the stops obtained would be false ones.

In order to reduce the chances of a menu being invalid, it was desirable that it should contain only a few links. However the use of a menu with a small number of links almost inevitably led to the generation of a large number of "false stops", making the subsequent task of identifying the correct "stop" much more time consuming and difficult.

In last month's article, the photo of the front of the Bombe showed the face of the rows of drums. Each vertical set of three drums together with a reflector plugboard on the back left hand end of the machine is the electrical equivalent of a German Enigma machine. A set of three drums are often referred to as Letchworth Enigmas. (Named after the location of the company that built them.)

There were 36 such Letchworth Enigmas with their external connection brought out to the rear of the machine. The top drums go around the fastest but in fact are the equivalent to the Enigma's slow, left-hand wheel. There was a good reason for this but it would be necessary to think like Alan Turing to understand it. The top drums of each three wheel set rotate continuously with the middle ones stepping by ratchet acting after the top drums have performed 26 electrical tests. The bottom drum steps again by ratchet action at the time as the middle ones but only once in every rotation of the middle drums.

On the far right are three indicator drums. These are permanently attached to the machine and when the machine "stops" they indicate a possible condition that after further processing might lead to the setting used by the Germans on their Enigma machine to encipher the text. They would be set to ZZZ before starting a run. If during a run no "stop" were found the machine would then return to ZZZ and come to a halt having carried out 26X26X26 unsuccessful tests.

After the complete Enigma key had been found, all of the messages in the corresponding batch could be easily deciphered. This work was carried out by British

TypeX

Type-X cipher machines that had been modified to emulate Enigma machines. If the settings were correct, entering the enciphered message would produce the original text (in German of course). The volume of traffic in the Decoding Room was eventually so great that hundreds of women were needed to operate those machines.

Remember the Bombe was not a computer; it did not do numerical calculations.

Part 4 — The Colossus Code Breaking Machine

As the Germans ramped up their war efforts in 1940 and enciphered message traffic thus increased, it became apparent that the hunt-and-peck, see the letter, write it down, and send it by Morse code technique using the Enigma was not fast enough. And even though the Germans were convinced that the Enigma code was unbreakable, they developed a new machine that promised to be even more secure and faster: the **Lorenz**.

This new system introduced by the German High Command was based on the sophisticated Lorenz SZ40 (later replaced by the more advanced Lorenz SZ42). These

Courtesy of Tony Sale, Bletchley Park

The Lorenz SZ42

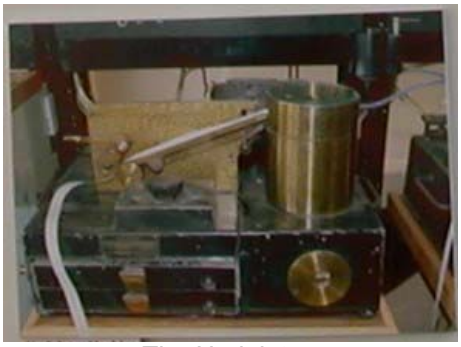
machines had twelve cipher wheels compared to the four or five wheels used with the Enigma and were used in conjunction with teleprinter equipment (like those seen at the Museum of Communications last March 28th) of the type then commonly employed by many countries for their communications.

The German High Command began using the new cipher system in 1941 to communicate with the Field Marshals who were in command of the Armies operating in different parts of Europe. The teleprinter equipment was used in conjunction with radio links that radiated out from Germany like the spokes of a wheel, to numerous military headquarters located in occupied and axis countries.

The British had to develop a way to intercept and decipher these important messages. Throughout 1941, the Germans had been conducting numerous experiments and increasing their use of radio teleprinter communications. So much so that it required opening a new "Y" Station at Knockholt, England for the intercepting of this type of traffic.

Teleprinters send and receive characters at approximately (in Europe) 66 words per minute using the ITA2 code commonly referred to as "Baudot" by hams that use RTTY and uses special function keys, for example, Line Feed and Shift. The direct connection to a radio was not possible because the Lorenz SZ42 acted upon the five function keys so letters can be changed into these invisible control codes.

Therefore, some other method had to be adopted to record the encrypted message from the radio receiver. This was achieved by using a piece of apparatus known as an ***undulator***. This is basically a pen



The Undulator

recorder that traced out the telegraph signals onto a narrow paper tape referred to as a "slip".

The breaking of this very complex cipher was one of the greatest triumphs for the code breakers at Bletchley Park. Their remarkable success was largely based on a combination of mathematical genius and the pioneering developments in electronic engineering that culminated in the building of "Colossus", arguably the world's first digital computer.

How the Lorenz Machine Operated

In the International teleprinter code each letter was represented by a group of five electrical "impulses" that today would be represented as a five bit binary number made up of 0s and 1s. For example the letter "A" would be represented by the code group 1 1 0 0 0.

The Lorenz Machine enciphered each letter of plain-text by altering in a pseudo-random way some (or all) of the five "impulses" of the teleprinter code group representing it thus generating the teleprinter code group of the cipher letter. At the receiving station a second Lorenz machine would automatically change the five "impulses" in the teleprinter code group of the cipher letter back to those in the teleprinter code group of the original plain-text message.

In effect the machine generated a pseudo random letter known as a "key" letter that was then "added" to the plain-text letter to produce the corresponding letter of cipher, this process being carried out on each letter of the plain-text message. The key changes with each lettered pressed.

To communicate between two locations it was necessary to have a Lorenz machine at each end of the communications link, with the twelve cipher wheels adjusted to the same set of starting positions (just as the Enigma did), so that they would generate identical sequences of "key" letters. At the sending station the first machine "added" the "key" letters to the plain-text letters to produce the cipher letters for transmission.

At the receiving station the second Lorenz machine "added" the same sequence (or stream) of "key" letters to the received sequence of cipher letter. As a consequence of

the particular rules used for the "adding" process, the resulting output would be the original sequence of letters of plain-text.

The complex way in which the cipher wheels moved in the machine resulted in sequences of "key" characters that were almost random (a different key for each letter pressed) and believed by the German cipher experts to virtually unbreakable.

Here is an example showing the encipherment and decipherment of the letter "G":

Enciphering:	Teleprinter code
Plain text letter: G	.. x .. x x
Machine generated *key* letter: D	x .. .. x ..
Cipher letter(= sum Plain text + *key*):	x x .. .. x (= W)
Deciphering:	
Received cipher letter: W	x x x
Machine generated *key* letter: D	x .. .. x ..
Plain text letter (= sum Cipher + *key*)	.. x .. x x (=G)

How the Lorenz machine was emulated

In August 1941, as a result of a lapse in security on the part of two German cipher clerks, two long messages were intercepted that had been enciphered *using the same sequence of key letters*. The receiving operator responded after the first message something to the effect, "Hey dummkopf, I didn't get all of that, send it again." The second time however, because it was a very long message to type, the operator started to make abbreviations to speed up the job. From these two message and after a great deal of hard work, the basic design of the Lorenz machine was deduced. It then became possible to build a machine in the UK (known as "**Tunny**") to emulate the German machine.

Finding the Wheel Settings

Whereas the Bombe was adequate to determine the wheel settings for the 3 wheel Enigma, determining the 12 wheel settings of the Lorenz machine was far beyond its capability.

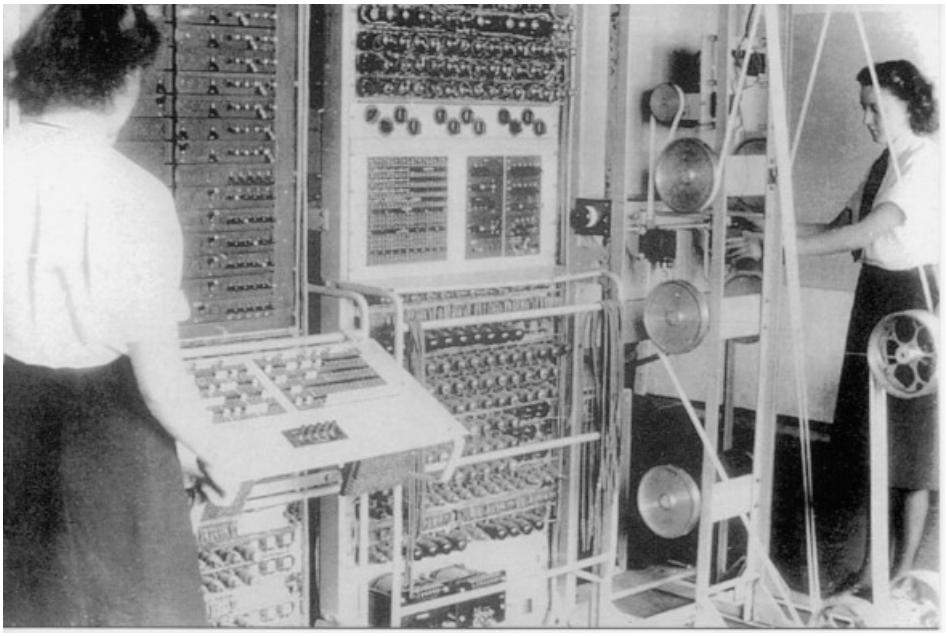
The Tunny

Building on the early work of mathematician Alan Turing in developing a "computing machine" , his mentor Max Newman designed a machine to find the settings, the first of which was built by the Post Office Research Station at Dollis Hill. Code named the "**Heath Robinson**", it was notoriously ill-tempered, prone to breaking down and catching on fire. Worse, the teleprinter tapes that were central to its design tended to tear. Ultimately, Newman and an electronics engineer Dr. Tommy Flowers overcame the technical difficulties that plagued the Heath Robinson. The result was the much more efficient, 1,500 electronic tube, aptly named, **Colossus**.

Tommy Flowers had the brilliant idea of producing the trial key streams electronically thus avoiding the tape synchronization problem of machines that used two tapes. Now only one tape was required (the intercepted enciphered text).

An immediate criticism was the number of vacuum tubes (valves to the Brits) needed; over 500 for the key stream generators and 1,500 for the whole machine. However, Flowers knew from his pre-war Post Office experience that vacuum tubes were very reliable *providing that* they were never switched off and this was done with Colossus. Once it was assembled and turned on, it was never switched off and it was extremely reliable.

The various parts of Colossus were designed and built at Dollis Hill from April 1943 onwards. In February 1944 it did its first live run



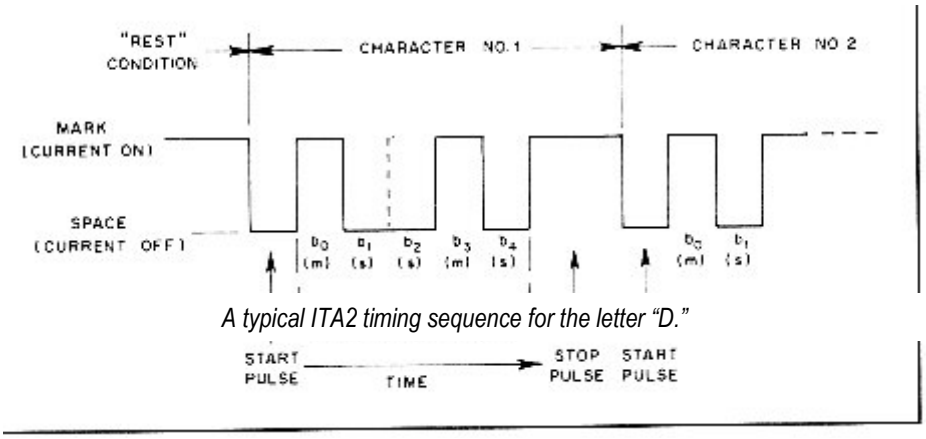
Operating the "Colossus"

against an intercepted tape. It was immediately successful in finding the Lorenz wheel settings and much to everyone's amazement the answers came out the same when the runs were repeated.

Part 5 — From the Radio Signal to the Deciphered Message

When the Germans switched from using the Enigma to using the Lorenz SZ42 in about 1941, the time to decipher the enciphered message increased dramatically. Thus a new method of handling the deciphering was required.

Furthermore the radio signals received were no longer Morse code but were what we now call International Teletype Alphabet 2 (ITA2), often referred to as Baudot by ham radio operators here. Sent by teleprinters the signals were much too fast to copy manually by the wireless operators. (While military trained radio operators could copy code at extremely fast speeds, they operated with whole words and phrases that were not trained in German.) It produced letters, numbers, and a few punctuation symbols with a five bit code. The figure



A typical ITA2 timing sequence for the letter "D."

shows what would be a trace seen on an oscilloscope.

As mentioned last time, a device known as the *undulator* was connected to the radio receiver to record the signals. This is basically a pen recorder that traced out the telegraph signals onto a narrow paper tape, referred to as a "slip", as the audio tones varied. The Germans used six audio tones. 3 for mark (current on) and 3 for space (current off). This gave some degree of safety against selective fading on the radio signals.

Since there was only one chance of obtaining a copy of a message, every effort was taken by

A Recreated Listening Station at BP showing 5 (count 'em) RCA AR88s!

the staff to get the most accurate one possible. Diversity reception was used extensively. This involved the use of two or three receivers at each operating position. The majority of the receivers were the RCA AR88.

The receivers were connected to different rhombic antennas in the antenna farm, selected by the operator via the antenna patch rack. Rhombics were chosen for their low angle of radiation, unidirectional properties and a certain degree of gain over a half-wave dipole. The

Close-up of the RCA AR88—A true boat anchor weighing 100 pounds

largest of these ranged between 700 and 1000 feet across their major axis. These were supported by 105-foot high wooden lattice towers. A number of smaller rhombics were erected on 70-foot high steel masts. Between them, these antennas covered the frequency range of 2—16 MHz.

The outputs of the receivers were connected to a high-speed bridge that automatically selected the receiver offering the best reception and then on to the undulator. (A "voter" in today's repeater parlance.)

The undulator "slips" were read by women operators, usually WRNS (aka Wrens), who mentally converted into the proper charac-

A Perforator Machine

ters and put onto a paper tape using a perforating machine.. They quickly became very adept at recognizing each of the 32 possible characters.

Slip reading was a thankless and tedious task. The women had to memorize every unique trace

each character made on the slip and experienced slip readers could read at up to 60 characters per minute. At Knockholt in Kent, England, the main listening station, there were about 300 slip readers.

All out efforts were made to produce an accurate copy of the message since Colossus was intolerant of too many errors. Only 6 errors in every 1000 characters was the maximum allowed. Each slip was read twice by different readers who would compare the two perforated tapes produced. Any errors had to be corrected by referring back to the slip. One of the tapes was chosen to become the corrected copy, which would have the errors cut out and correct sections placed in. The corrected copy was then passed through a tap transmitter connected to a re-perforator. This produced a master tape, which again was checked against the corrected copy.

A printed copy was also required by the Tunny operator at Bletchley. If one had been obtained at the time of reception it was checked against the undulator slip and any errors corrected. If no suitable copy had been produced during reception then one was obtained from the master tape using a shiftless teleprinter connected to a tape reader. The printed copies were normally sent to Bletchley by dispatch rider.

The master tape was passed through two tape transmitters that sent the cipher text over two separate teleprinter landlines to Bletchley. Here the text was received on two re-perforating machines. As the two tapes were being produced, every so often a operator would check them against each other, looking for errors. Any differences between the two tapes would have to be referred back to Knockholt for checking.

Once two accurate tapes had been produced at Bletchley, one was selected for processing by Colossus. Referring to the photo of the Colossus to the right you can see the paper tape that was used.

The Colossus Paper Tape "Bedstead"

It is loaded as an endless loop onto the "bedstead" on the right hand side of Colossus. Here it was read optically at 5,000 characters per second into Colossus.

Colossus then tried various possible Lorenz wheel starts by stepping through the various possible settings, looking for the maximum score that appeared on the lamp panel on the left hand side of Colossus. When the highest score

had been found it was printed on the typewriter together with the wheel setting it found.

A more complete description of the design and operation of the Colossus is beyond the scope of this article and the interested reader is challenged to research this further.

When all 12 Lorenz wheel positions were found, they were entered into the Tunny, which emulated the German Lorenz, to decipher the message. It took about 8 hours to find all 12 wheel setting.

With the wheel settings in hand, the Tunny operator could set up her machine and feed in the message to be deciphered. Last month's article showed a photo a reconstructed Tunny.

Grateful acknowledgement is given to the staff and volunteers at Bletchley Park for information and displays of equipment used by the code breakers.

An interesting film by the Polish about the work of the Poles on breaking the Enigma machine is "The Enigma Secret", which can be rented from Netflix. Be sure to have your DVD player set to display subtitles.

For further reading see:

Delusions of intelligence : Enigma, Ultra and the end of secure ciphers, R. A. Ratcliff. New York : Cambridge University Press, c2006.

The Secret Wireless War, G. Pidgeon, 2003

GCHQ, Nigel West, 1986

Ian Fleming, Andrew Lycett, 1995

Station X, Michael Smith, 1998

Ultra Goes to War, Ronald Lewin, 1978