Lorenz and Colossus

Anthony E. Sale
Former Museums Director, Bletchley Park

1. The German cipher system

The German Army High Command asked the Lorenz company to produce for them a high security teleprinter cipher machine to enable them to communicate by radio in complete secrecy.

The Lorenz company designed a cipher machine based on the additive method for enciphering teleprinter messages invented in 1918 by Gilbert Vernam in America.

The Vernam system enciphered the message text by adding to it, character by character, a set of obscuring characters thus producing the enciphered characters which were transmitted to the intended recipient. The simplicity of Vernam's system was that if the obscuring characters were added in a rather special way (known as Modulo 2 addition) then exactly the same obscuring characters added in the same way to the received enciphered characters, cancelled out the obscuring characters and left the original message characters which could then be printed.

Vernam proposed that the obscuring characters should be completely random and pre-punched onto paper tape to be consumed character by character in synchronism with the input message characters. Such a cipher system using purely random obscuring characters is unbreakable.

The difficulty was, in a hot war situation, to make sure that the same random character tapes were available at each end of a communications link and that they were both set to the same start position. The Lorenz company decided that it would be operationally easier to construct a machine to generate the obscuring character sequence. Because it was a machine it could not generate a completely random sequence of characters. It generates what is known as a pseudo random sequence. Unfortunately for the German Army it was more "pseudo" than random and that was how it was broken.

The amazing thing about Lorenz is that the code breakers in Bletchley Park never saw an actual Lorenz machine until right at the end of the war but they had been breaking the Lorenz cipher for two and a half years.

2. The first intercepts

The teleprinter signals being transmitted by the Germans enciphered using Lorenz were first heard in early 1940 by a group of policemen on the South Coast who were listening out for possible German spy transmissions from inside the UK.

Brigadier John Tiltman was one of the top code breakers in Bletchley Park and he took a particular interested in these enciphered teleprinter messages. They were given the code name "Fish" and the messages which, as was later found out, were enciphered using the Lorenz machine were known as "Tunny". Tiltman knew of the Vernam system and soon identified these messages as being enciphered in the Vernam manner. Because the Vernam system depended on addition of characters, Tiltman reasoned if the operators had made a mistake and used the same Lorenz machine starts for two messages (a Depth), then by adding the two cipher texts together character by character, the obscuring character sequence would disappear. He would then be left with a sequence of characters each of which represented the addition of the two characters in the original German message texts. For two completely different messages it is virtually impossible to assign the correct characters to each message. Just small sections at the start could be derived but not complete messages.

3. The German mistake

As the number of intercepts, now being made at Knockholt in Kent, increased a section was formed in Bletchley Park headed by Major Ralph Tester and known as the Testery. A number of Depths were intercepted but

0-7695-0671-2/00 $10.00 © 2000 IEEE

not much headway had been made into breaking the cipher until the Germans made one horrendous mistake. It was on 30th August 1941 and a German operator had a long message of nearly 4,000 characters to be sent from one part of the German Army High command to another. Probably Athens to Vienna. He correctly set up his Lorenz machine and then sent a twelve letter indicator, using the German names to the operator at the receiving end. this operator then set his Lorenz machine and asked the operator at the sending end to start sending his message. After nearly 4,000 characters had been keyed in at the sending end, by hand, the operator at the receiving end sent back by radio the equivalent, in German, of "didn't get that--send it again".

They now both put their Lorenz machines back to the same start position. Absolutely forbidden, but they did it . The operator at the sending end then began to key in the message again, by hand. If he had been an automaton and used exactly the same key strokes as the first time then all the interceptors would have got would have been two identical copies of the cipher text. Input the same - machines generating the same obscuring characters - same cipher text. But being only human and being thoroughly disgusted at having to key it all again, the sending operator began to make differences in the second message compared to the first.

The message began with that well known German phrase SPRUCHNUMMER, "message number" in English. The first time the operator keyed in S P R U C H N U M M E R. The second time he keyed in S P R U C H N R and then the rest of the message text. Now NR means the same as NUMMER what's the difference? It meant that immediately following the N the two texts were different but the machines were generating the same obscuring sequence, therefore the cipher texts were different from that point on.

The interceptors at Knockholt realised the possible importance of these two messages because the twelve letter indicators were the same. They were sent post haste to John Tiltman at Bletchley Park. Tiltman applied the same additive technique to this pair as he had to previous Depths. But this time he was able to get much further with working out the actual message texts because when he tried SPRUCHNUMMER at the start he immediately spotted that the second message was nearly identical to the first. Thus the combined errors of having the machines back to the same start position and the text being re-keyed with just slight differences enabled Tiltman to recover completely both texts. The second one was about 500 characters shorter than the first where the German operator had been saving his fingers. This fact also allowed Tiltman to assign the correct message to it's original cipher text,

Now Tiltman could add together character by character, the corresponding cipher and message texts revealing for the first time a long stretch of the obscuring character sequence being generated by this German cipher machine. Not knowing how the machine did it, but this was what it was generating!

4. The denouement

John Tiltman then gave this long stretch of obscuring characters to a young chemistry graduate, Bill Tutte recently come to Bletchley Park from Cambridge.

Bill Tutte started to write out the bit patterns from each of the five channels in the teleprinter form of the string of obscuring characters at various repetition periods. Remember this was BC, "Before Computers", so he had to write out vast sequences by hand. When he wrote out the bit patterns from channel one on a repetition of 41, various patterns began to emerge which were more than random. This showed that a repetition period of 41 had some significance in the way the cipher was generated. Then over the next two months Tutte and other members of the Research section worked out the complete logical structure of the cipher machine which we now know as Lorenz. This was a fantastic tour de force and at the beginning of 1942 the Post Office Research Labs at Dollis Hill were asked to produce an implementation of the logic worked out by Bill Tutte and co. Frank Morrell produced a rack of uniselectors and relays which emulated the logic. It was called "Tunny". So now when the manual code breakers in the Testery had laboriously worked out the settings used for a particular message, these settings could be plugged up on Tunny and the cipher text read in. If the code breakers had got it right, out came German. But it was taking four to six weeks to work out the settings. This meant that although they had proved that technically they could break Tunny, by the time the messages were decoded the information in them was too stale to be operationally useful.

5. The machine age

The mathematician Max Newman now came on the scene. He thought that it would be possible to automate some parts of finding the settings used for each message. He approached TRE at Malvern to design an electronic

machine to implement the double delta method of finding wheel start positions which Bill Tutte had devised. The machine was built at Dollis Hill and was known as Heath Robinson after the cartoonist designer of fantastic machines.

There were problems with Heath Robinson keeping two paper tapes in synchronism at 1,000 characters per second. One tape had punched onto it the pure Lorenz wheel patterns that the manual code breakers had laboriously worked out. The other tape was the intercepted enciphered message tape. The double delta cross correlation measurement was then made for the whole length of the message tape. The relative positions then moved one character and the correlation measurement repeated. The code breaker was looking for the relative position which gave the highest cross correlation score which hopefully corresponded with the correct Lorenz wheel start position.

Heath Robinson worked well enough to show that Max Newman's concept was correct. Newman then went to Dollis Hill where he was put in touch with Tommy Flowers who was the brilliant Post Office electronics engineer who designed and built Colossus to meet Max Newman's requirements for a machine to speed up the breaking of the Lorenz cipher.

Tommy Flower's major contribution was to propose that the wheel patterns be generated electronically in ring circuits thus doing away with one paper tape and completely eliminating the synchronisation problem. This required a vast number of electronic valves but Tommy Flowers was confident it could be made to work. He had, before the war, designed Post Office repeaters using valves. He knew that valves were reliable provided that they were never switched on and off. Nobody else believed him!

Colossus design started in March 1943. By December 1943 all the various circuits were working and the 1,500 valve Mk1 Colossus was dismantled shipped up to Bletchley Park and assembled in F Block over Christmas 1943. The Mk1 was operational in January 1944 and successful on its first test against a real enciphered message tape.

6. The contribution to D Day

Colossus reduced the time to break Lorenz messages from weeks to hours and just in time for messages to be deciphered which gave vital information to Eisenhower and Montgomery prior to D Day. These deciphered Lorenz messages showed that Hitler had swallowed the deception campaigns, the phantom army in the South of England, the phantom convoys moving east along the channel, that Hitler was convinced that the attacks were coming across the Pas de Calais and that he was keeping Panzer divisions in Belgium. After D Day the French resistance and the British and American Air Forces bombed and strafed all the telephone and teleprinter land lines in Northern France, forced the Germans to use radio communications and suddenly the volume of intercepted messages went up enormously. The Mk1 had been rapidly succeeded by the Mk2 Colossus in June '44 and eight more were quickly built to handle the increase in messages. The Mk1 was upgraded to a Mk2 and there were thus ten Mk2 Colossi in the Park by the end of the war. By the end of hostilities 63 Million characters of high grade German messages had been decrypted, an absolutely staggering output from just 550 people at Bletchley Park, plus of course the consideable number of interceptors at Knockholt, with backups at Shaftsbury and Coupar in Scotland.

7. The Colossus Computer

Each of the ten Colossi occupied a large room in F Block or H Block in Bletchley Park. The racks were 90 inches, (2.3m), high of varying widths. There were eight racks arranged in two bays about 16ft (5.5m) long plus the paper tape reader and tape handler (known as the bedstead). The front bay of racks, spaced 5ft (1.6m) from the rear bay, comprised from right to left, the J rack holding the master control panel, the plugboard some cathode followers and the AND gates. Next came the K rack which contained the very large main switch panel together with the very distinctive sloping panel at the front which was a duplicate patch panel for the thyratron rings. Next came the S rack which held the relays used for buffering counter output and making up the typewriter drive logic. The left hand rack at the front was the C rack which held the counter control logic on the front and the decade counters on the back.

The rear bay of Colossus contained four racks, the R rack holding the staticiser and delta boards for the paper tape reader output and the K and S wheel thyratron ring outputs, the M rack for the M wheel staticisers and S wheel motion logic. The very large W rack held, on one side all the thyratrons making up the wheel rings, 501 in all, and on the other side the 12 thyratron ring control panels. Also on the W rack were the link boards for the wheel patterns and the uniselectors for setting wheel start positions. The end rack of the back bay held the power

packs. These were 50 volt Westat units stacked up in series to give +200 volts to -150 volts. The total power consumption was about 5 Kilowatts most of which was to the heaters of the valves.

The circuit layout was all surface mounting on metal plates bolted to the racks. The valve holders were surface mounting with tag strips for the components. This form of construction had much to commend it, firstly both sides of a rack could be used, secondly wiring and maintenance were very easy and lastly cooling of the valves was expedited by them being horizontal.

8. How Colossus worked

Colossus read teleprinter characters, in the international Baudot code, at 5,000 characters per second from a paper tape. These characters were usually the intercepted cipher text which had been transmitted by radio. The paper tape was joined into a loop with special punched holes at the beginning and end of the text.

The broad principle of Colossus was to count throughout the length of the text the number of times that some complicated Boolean function between the text and the generated wheel patterns had either a true or false result. At the end of text the count left on the counter circuits was dumped onto relays before being printed on the typewriter during the next read through the text, an early form of double buffering.

Colossus had two cycles of operation. The first one was controlled by the optical reading of the sprocket holes punched between tracks 2 and 3 on the paper tape. The sprocket signal was standardised to 40 microseconds wide. The optical data from the paper tape was sampled on the back edge of the standardised sprocket pulse as was the outputs from the rings of thyratrons representing the Lorenz wheel patterns. The result of the logical calculation was sampled on the leading edge for feeding into the counter circuits.

The second cycle of operations occurred at the beginning and end of the text punched onto the paper tape. The paper tape was joined into a loop and special holes were punched just before the start of text between channels three and four (called the start) and just after the end of text between channels four and five (called the stop). This long cycle of operations began with the electrical signal from the photocell reading the stop hole on the tape. This stop pulse set a bistable circuit which stayed set until the optical signal from the start hole was read. The setting of this bistable thus lasted for the duration of the blank tape where the text was joined into a loop, typically about 100 millisec. The first operation after the stop pulse was to release any settings on the relays from the previous count. Next the new count was read onto the relays. Then the counters and the thyratron rings were cleared and then the thyratron rings were struck at the next start point to be tried. When the bistable was reset by the start pulse, sprocket pulses were released to precess the thyratron rings, to sample the data read from the paper tape and to sample the calculation output to go to the counters.

The various components of Colossus were the optical reader system, the master control panel, the thyratron rings and their driver circuits, the optical data staticisors and delta calculators, the shift registers, the logic gates, the counters and their control circuits, the span counters, the relay buffer store and printer logic.

9. The optical reader system

In order to break the Lorenz codes in a reasonable time the cipher text had to be repeatedly scanned at very high speed. This meant at least 5,000 characters per second and in the 1942 this implied hard vacuum photocells to optically read the holes in the paper tape. The smallest photocells available were some developed for proximity fuses in anti aircraft shells. Six of these in a row meant an optical projection system to enlarge the image of the paper tape about 10 times. Dr Arnold Lynch designed the paper tape reader and used slits cut into black card to form a mask in front of the photocells.

The output from the data channels went to the staticiser and delta circuits.

10. The master control panel

This was where the start and stop pulses from the optical reader set and reset the bistable. Monostable delay circuits generated the voltage waveforms for releasing the relays, for staticising the counters, for resetting the counters and thyratron rings, and for striking the rings. Gate circuits controlled the flow of sprocket pulses.

11. The thyratron rings and their driver circuits

These circuits were the most complex on Colossus. Thyratrons are gas filled triodes which strike a discharge arc between anode and cathode when the grid voltage is

raised to allow electrons to flow. This discharge when struck continues quite independent of the grid voltage. Thus the thyratron acts as a one bit store. It can only be switched off by driving both the anode and the grid negative with respect to the cathode. To construct a shift register with thyratrons requires that the striking of the next thyratron in the ring also quenches the previous thyratron. This leads to a biphase circuit with anodes of alternate thyratrons connected together and the grid voltage partially biased by the cathode voltage of the previous thyratron.

The complication arises when a Lorenz wheel contains an odd number of setting lugs. The thyratron ring controller for this requires a complete set of circuits to handle just the odd thyratron in order to get back to the biphase circuits for the rest of the ring. The thyratrons in a ring conduct sequentially stepped round by the sprocket pulses. Each thyratron cathode is brought out to a patch panel which allows the cathode pulse to be connected to a common output line when a link is plugged into the patchboard. Thus as the ring precesses round a sequence of pulses appears on the common output line. By selecting the link positions this sequence can replicate the mechanical lugs set on the Lorenz wheel. Alongside the patch panel is a Uniselector which selects the thyratron cathode to which the ring strike pulse goes. This is the start position of the ring when sprocket pulses come in at the start of text.

The common line output went to the staticiser and delta circuits.

12. The staticisors and delta circuits

These circuits take the raw signals from the paper tape reader and the thyratron rings, sample them on the back edge of the clock pulse and set them to standard voltages of +- 80 volt. Also on these boards are circuits giving a delay of one clock pulse. This is achieved with integrator capacitors which "hold" the previous data signal for long enough for it to be sampled on the next sprocket pulse. This delayed signal is available as an output but also on the board is an adder circuit which produces the delta signal, i.e. a one when current data is different from previous and a zero when current equals previous.

13. The shift registers

These are the same circuits used as used on the delta boards, just integrators sampled on the next sprocket pulse. Up to 5 shift elements could be connected in cascade giving a 5 bit shift register. This is thought to be the first recorded design or use of a shift register. Some of the computational algorithms used this window on pervious data to improve the cross correlation measurement.

14. The logic gates

Colossus was provided with AND and OR gates which could be plugged together in any combination.

15. The counter and counter control circuits

The decade counter circuits were based on a pre-war design by Wynn-Williams. They used a divide by two circuit followed by a ring of five pentodes. Four decades were required for each of the five counters used and each control circuit covered four decades of counters. The inputs to the control circuits were the output from the logic gates, the sprocket pulse for strobing and the reset pulse from the master control panel. Also on the control panels were comparator circuits between the outputs of the decade counters and switches on another panel. These switches could be set to any number in the range 0 to 9999. The output of the comparator could be included in the logic calculations thus for instance suppressing printing of scores below a set value.

16. The span counters

These were the same design of counters and counter control circuits with switches on another panel which could be set in the range 0 to 9999. The purpose of the span counters was to be able to ignore sections of the cipher text which were corrupted, possibly due to fading radio signals. The comparator output was used to gate the sprocket pulses which went to the main counter controllers, cutting off these pulses stopped the sampling of the logic calculation and thus ignored the section of text covered by the span counters.

17. The relay buffer store and printer logic

Latching relays held the ending count on the decade counters. The start positions of the thyratron rings and the count for the pervious run through the text are clocked out sequentially onto the typewriter by the printer relay and uniselector logic.

18. Programming Colossus

Programming of the cross correlation algorithm was achieved by a combination of telephone jack plugs and cords and switches. The main plug panel was on the rack nearest to the paper tape reader. The direct and delta signals from the paper tape reader and the K wheel thyratron rings were on this panel. The changeover from direct to delta could also be achieved by switches. Also on the main plug panel were the input and output sockets for the AND gates and the so called "Q" sockets which took the calculated output to the main switch panel on the next rack to the left. This very large switch panel allowed signals to be combined through further logic gates and the results switched to any of the five result counters.

As an example take the simple double delta algorithm as devised by Bill Tutte. This requires two wheel to be run simultaneously so take K4 and K5.

First the delta outputs from channel 5 from the paper tape reader is combined in an AND gate with the delta output of the K5 thyratron ring, then this result is ANDed with the AND output of delta channel 4 and the delta output of the K4 thyratron ring. This result is plugged to Q1 and on the switch panel Q1 is switched to counter 1. The output can be negated before being counted so that the count can represent either the number of times the double delta calculation equals one or zero.

19. The end of Colossus

After VJ Day, suddenly it was all over. Eight of the ten Colossi were dismantled in Bletchley Park. Two went to Eastcote in North London and then to GCHQ at Cheltenham. These last two were dismantled in about 1960 and in 1960 all the drawings of Colossus were burnt, and of course its very existence was kept secret.

In the 1970's various information began to emerge about Colossus. Professor Brian Randell of Newcastle University started researching Colossus. Dr Tommy Flowers and some of the other design engineers gave papers in the 1980's describing Colossus in fairly general terms.

20. The rebuild

When I and some colleagues started, in 1991, the campaign to save Bletchley Park from demolition by property developers, I was working at the Science Museum in London restoring some early British computers. I believed it would be possible to rebuild Colossus. Nobody believed me. In 1993 I gathered together all the information available. This amounted to the eight 1945 wartime photographs taken of Colossus plus some fragments of circuit diagrams which some engineers had kept quite illegally, as engineers always do!

I spent 9 months poring over the wartime photographs using a sophisticated modern CAD system on my PC to recreate the machine drawings of the racks. I found that sufficient wartime valves were still available as were various pieces of Post Office equipment used in the original construction.

In July 1994 His Royal Highness The Duke Of Kent opened the Museums in Bletchley Park and inaugurated the Colossus Rebuild Project. At that time I had not managed to obtain any sponsorship for the project and my wife Margaret and I decided to put our own money into it to get it started. We both felt that if the effort was not made immediately there would be nobody still alive to help us with memories of Colossus. Over the next few years various private sponsors came to our aid and some current and ex Post Office and radio engineers formed the team that helped me in the rebuild.

21. The switch on

By 1995 the optical paper tape reader was working, (helped by the memories of Dr Arnold Lynch who designed it in 1942) and the basic circuitry of Colossus had been recreated. Colossus first worked at two bit level (out of the five bit channels from the paper tape). HRH The Duke of Kent returned to the Park on 6th June 1996 to switch on the basic working Colossus. This was a marvellous occasion with Dr Tommy Flowers present and a large number of the people who worked at Knockholt, in the Testery and the Newmanry during the war.

One reason for wanting to get Colossus working in 1996 was that for far too long the Americans have got away with the myth that their ENIAC computer was the first in the world. It was not, but they got away with it because Colossus was kept secret until the 1970's. As 1996 was the 50th anniversary of the switch on of ENIAC I made sure that Colossus was rebuilt and working in Bletchley Park, just as it was in 1944. There has been a stunned silence from across the water!

0-7695-0671-2/00 $10.00 © 2000 IEEE

22. The American information

One ironic twist to the Colossus story is that most of the information about how Colossus was used has come from America. In 1995 the American National Security Agency (equivalent to GCHQ) was forced by application of the Freedom of Information Act to release about 5,000 World War II documents into the National Archive. The listing of these documents was put onto the Internet and I quickly obtained a copy of the list. When I scanned this I was amazed to see titles like "The Cryptographic Attack on FISH". I managed to get copies of these documents only to find that they were reports written by American service men seconded to Bletchley Park when America entered the war. The most important one was written by Albert Small and is a complete description of Colossus code breaking. Having this report has enabled us to work out the function of many more of the circuits and programme switches on Colossus. We have now, we think, incorporated nearly all the circuits and although there may still be some parts which cannot be worked out, we think we have about 90% of Colossus correct and working.

23. The performance of Colossus

Colossus is not a stored programme computer. It is hard wired and switch programmed, just like ENIAC. Because of its parallel nature it is very fast , even by today's standards. The intercepted message punched onto ordinary teleprinter paper tape is read at 5,000 characters per second. The sprocket holes down the middle of the tape are read to form the clock for the whole machine. This avoids any synchronisation problems, whatever the speed of the tape, that's the speed of Colossus. Tommy Flowers once wound up the paper tape drive motor to see what happened. At 9,600 characters per second the tape burst and flew all over the room at 60 mph! It was decided that 5,000 cps was a safe speed.

At 5,000 cps the interval between sprocket holes is 200 microsecs. In this time Colossus will do up to 100 Boolean calculations simultaneously on each of the five tape channels and across a five character matrix. The gate delay time is 1.2 microsecs which is quite remarkable for very ordinary valves. It demonstrates the design skills of Tommy Flowers and Allen Coombs who re-engineered most of the Mk2 Colossus.

Colossus is so fast and parallel that a modern Pentium PC programmed to do the same code breaking task takes twice as long as Colossus to achieve a result!

24. Finally

The rebuilt and working Colossus can now be seen in the Museums at Bletchley Park which are open to the public every other weekend throughout the year. It is marvellous tribute to Tommy Flowers, Allen Coombs and all the engineers at Dollis Hill and a great tribute to Bill Tutte, Max Newman, Ralph Tester and all the code breakers involved at Bletchley Park. Not forgetting all the WRNS who operated and supported Colossus and the interceptors at Knockholt without whom there would have been no messages to break.

Acknowledgements

I would like to thank my wife Margaret for agreeing to the use of our own money to start up the project and for her continuing support and encouragement. The financial sponsors are: A E & M D Sale, Mr Frank Morrell, The Mrs L D Rope Third Charitable Settlement, Mr Keith Thrower OBE, and Quantel Ltd. Moreover, Charles Head (Blacksmiths), Billington Exports Ltd, and Claude Lyons Ltd contributed by offering special low prices.

Thanks to the Bletchley Park Trust which has allowed free use of the room in H Block where Colossus has been rebuilt and to the many hundreds of individuals who have searched their garages and lofts and sent valves for Colossus.

The Colossus Team consisted of regulars Cliff Horrocks, David Stanley, Paul Bruton (deceased), John Lloyd and Bob Alexander; every other weekend members John Pether, Don Skeggs, Adrian Cole, and Ron Clayton; and intermittent helpers Don Grieg (deceased), Philip Hopkins, Richard Watson, Derek Turton, and Mark Hyman.

Gil Hayward, the original designer of Mk2 Tunny, turned some 600 pattern plugs and modified over 1,000 octal valve bases.