

The Colossus of Bletchley Park

At Bletchley Park, home of the UK's top-secret code-breaking activities in the Second World War, work is under way to rebuild Colossus, the machine that helped break the signal traffic of the German high command. **Tony Sale**, director of the Colossus rebuild project, describes the origins of this remarkable machine and the task of restoring it to life

During the Second War World, Bletchley Park in Bedfordshire, the UK centre for codebreaking, was responsible for a stream of priceless intelligence on the plans of the German military. So crucial was this work to the success of the Allied war effort that the very existence of Bletchley Park was kept secret until 1974.

In 1976, Prof. Brian Randell¹ revealed perhaps the most remarkable of Bletchley Park's secrets, with the announcement of a pioneering 2500-valve programmable logic calculator used to break the cipher messages of the German army high command. Called Colossus because of its unprecedented size, this extraordinary machine was instrumental in shortening the war, exposing Hitler's intentions in the build-up to D-Day in 1944.

Ten, or possibly 11, machines were built, and in sheer scale they completely eclipsed the American Eniac computer, which they predated by some two years.

The secrecy surrounding Colossus meant that it had no direct influence on the development of computers as we know them.

However, by demonstrating that a very large collection of electronic valves could be made to work together with great reliability, its indirect influence was

considerable. When Alan Turing came to put together his revolutionary proposals for the ACE computer, he knew that his design was eminently feasible because he had seen much larger machines working at Bletchley Park.

Since Prof. Randell's 1976 revelations, additional information has gradually appeared on Colossus. Detailed photo-

saving Bletchley Park from commercial development and seemingly inevitable destruction. It was at this point that the idea of rebuilding Colossus was born.

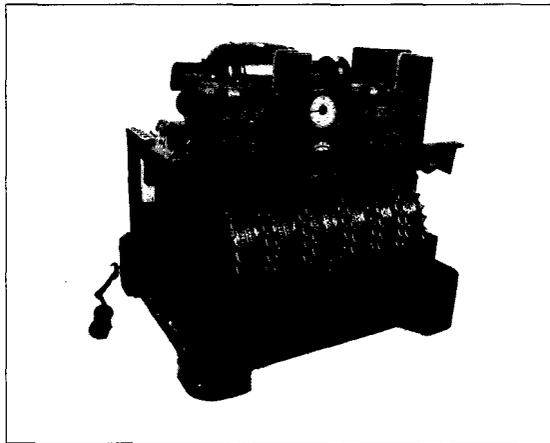
We were almost too late. Many of the original designers, builders and maintenance men had died, and of those still alive, all were in their 70s and 80s. No matter how urgently we wished to press ahead with building, we had first to prepare the ground with a substantial research programme into the origins and operation of Colossus.

Origins

The German military's offensive strategy, the Blitzkrieg, depended on the close and secure co-ordination of air and ground forces. This highly innovative tactic was made possible by the invention of easily portable radio sets, but relied on a large amount of radio traffic. Hence effective cipher systems were central to its co-ordination.

The Germans had adopted the Enigma machine as their front-line cipher system

as early as 1932. Enigma was the workhorse of German enciphering, but it was not the only machine used. The Lorenz SZ42 and the Siemens T52 were also employed, both machines using the Vernam cipher system to encipher teleprinter traffic. The Lorenz machine (Fig. 1) was used by the German army and



1 Lorenz machine showing the 12 wheels that control the enciphering process

graphs have been published, and the hardware details of the machine have all been declassified.

I was unaware of the role of Colossus until, in 1989, I discovered Prof. Randell's work while researching the history of early computers. In 1990 I became a founder member of a group dedicated to

Original character (A)	1	1	0	0	0
First set of enciphering wheels	1	0	0	1	1
Exclusive-OR result	0	1	0	1	1
Second set of enciphering wheels	0	0	0	0	1
Final exclusive-OR result (R)	0	1	0	1	0

the Siemens machine by the Luftwaffe.

Radio transmissions using these Vernam-based machines were intercepted in the UK from 1940, and were given the collective codename Fish. The Wehrmacht traffic on the Lorenz machine was designated by the codename Tunny. The enormous strategic importance of the Fish transmissions became apparent when traffic analysis revealed that they were messages between the German high command and the field commanders. Work on the decipherment problem, directed at the more strategically important Tunny traffic, began quickly under the direction of Brig. John Tiltman.

The Lorenz machine was based on 12 wheels, organised into two groups of five enciphering wheels and one group of two control wheels. Each wheel had a number of small pins on its circumference which were set by the operator, there being a total of 501 pins in all. These pins can be regarded as a sequence of 0s and 1s, depending on whether the operator sets the pin to on or off.

At a given position of all the wheels, one pin from each wheel would be in the operative position. An input character, punched in Murray code onto five-hole paper tape, was enciphered by successive exclusive-OR operations, first with the patterns given by the operative pins on the first group of five wheels, then with those on the second group of five wheels (Fig. 2). The first group of wheels moved each time a new character was input; the movement of the second group depended on the operative pins on the control wheels. Further details on the Lorenz machine are given in Reference 2.

By exploiting mistakes by German machine operators, John Tiltman was able to deduce that the cipher key was in two parts: the pin positions, changed once a day, and the wheel start positions, changed for every message. At first, laborious hand methods were used to determine the pin patterns and start positions of each wheel. By 1942, it was clear that mechanical aids would be required to decipher the large number of messages being intercepted.

This led, in late 1942, to 'Heath Robinson'-like machines whose task was

to find the wheel start positions used for a message. The intercepted enciphered message, punched onto five-hole paper tape, was made into a continuous loop. The hand-determined wheel-pin patterns were punched onto another paper tape, also formed into a loop.

These two tapes were then compared against each other using logic operations similar to those used in the original Lorenz machine, and scores kept of the results of the comparisons. The relative

**The machine was
difficult to
operate, and
accurate tape
synchronisation
very hard
to sustain**

positions of the tapes were stepped on one character after each complete pass around the loop to simulate a new start position for the wheels. Eventually, the correct wheel positions would be indicated by a small peak in the comparison scores. Unfortunately, the machine was difficult to operate, and accurate tape synchronisation very hard to sustain.

Dr. Tommy Flowers, at the GPO Research Laboratories at Dollis Hill, came up with the brilliant idea of producing the wheel pattern streams electronically, rather than reading them from a paper tape. This immediately removed the problem of synchronisation and allowed the intercepted enciphered paper tapes to be read at the unheard-of speed of 5000 characters per second.

They called the electronic machine Colossus, and the Mark 1 was developed during spring and summer of 1943. By the autumn, the various racks were working, and it was dismantled and taken from Dollis Hill to Bletchley Park, where it was reassembled over Christmas 1943. By

2 Process of enciphering letter A on a Lorenz machine

February 1944 it was being run against real intercepted tapes and it was successful on its first live run.

The success of the Mark 1 Colossus led to an immediate request for a more powerful Mark 2. With considerable foresight, Dr. Flowers had anticipated this move, and had components already in stock or on order. As a result the Mark 2 was ready by June 1944, in time for D-Day.

Design

The basic requirement for Colossus was high-speed repetitive reading of teleprinter traffic punched in Murray code onto five-hole paper tape, and the internal generation of sequences of digits corresponding to the patterns set on the wheels of a Lorenz machine. This pattern generation was synchronised to the sprocket holes read on the paper tape; these sprocket-hole pulses formed, in modern terms, the clock for the whole machine.

The generated patterns were then correlated with the intercepted cipher text on the paper tape. Accumulated scores were kept on decade counters and printed onto a typewriter after each complete read through the cipher text.

The Heath Robinson machines used a phase-modulated 25 kHz signal, a system which, although it used only about 50 valves, was extremely difficult to set up and maintain. In contrast, Dr. Flowers decided that Colossus should use DC signalling levels.³ Although this involved many more valves, he knew that they would be reliable provided that the heaters inside the valves were not switched on and off.

The wheel patterns were generated by rings of thyatron valves. In these only one thyatron could be on at a time. On each clock pulse the next thyatron in sequence was energised. The number of thyatrons in each ring corresponded to the number of positions on each wheel in the Lorenz machine. This meant 501 thyatrons in all.

One major problem was the heater consumption of the GTIC thyatrons, 6V at 1A for each valve. This necessitated 100A heater transformers, actually slung in the racks, to feed all the thyatrons.

Decade counters were required to accumulate the results of the logic operations between the generated patterns and the cipher text. Dr. Flowers decided to

3 Colossus with WRNS operators

base his design on a prewar design by Wynn-Williams at the Rutherford laboratories. The counters worked in bi-quinary mode with a divide-by-two bistable followed by a ring-of-five counter. This ring counter required close-tolerance $1\text{ M}\Omega$ resistors, achieved by ordering very large numbers of resistors and then sorting them into batches by exact value. The circuit diagram, which has survived, has a note saying that all megohm resistors in the bi-quinary circuit should be from the same batch number.

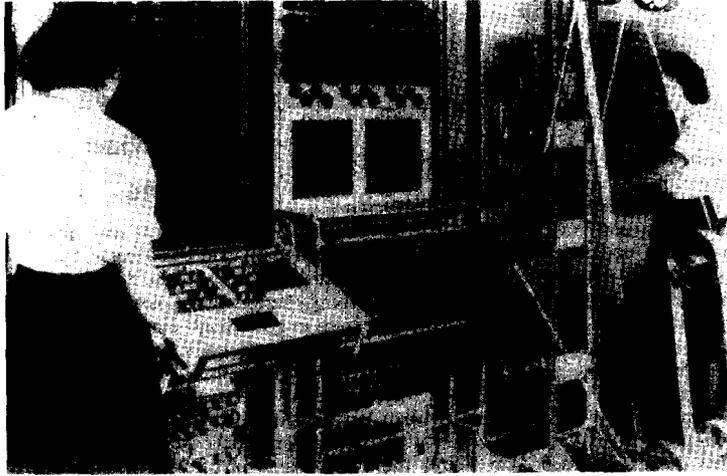
The valves used in the counters were Mullard EF36 pentodes or equivalent. This valve had two advantages. First, its heater consumption was very low, only 0.2 A at 6.3 V . Second, its suppressor electrode was brought out to a base pin, allowing the anode current to be switched by either grid or suppressor. This allowed AND or OR logic to be constructed easily.

In many ways, the optical system for reading the punched paper tape was the heart of Colossus, as it made the high processing speeds possible. The system was the responsibility of Dr. Arnold Lynch, an optics expert at Dollis Hill.

Dr. Lynch was never told the use to which his design was to be put. All he had was a brief specification detailing that punched paper tape was to be continuously read at at least 5000 characters per second, and that the output from the photoelectric cells was to be as nearly as possible a square wave for each hole read. He was given a large number of hard-vacuum photocells to use in the design, part of a stock of 10 000, originally intended for use as proximity detectors in anti-aircraft shells.

The cells formed the detectors for the data holes and the sprocket holes in the punched paper tape. Five data holes and one sprocket hole meant a row of six photocells. The optical system therefore comprised a high-power (50 W) lamp illuminating the paper tape through a collimator on one side, with a projecting lens giving a tenfold magnification on the other side, focusing an image of the paper tape onto the photocells.

Dr. Lynch realised that a mask was required in front of the photocells to achieve adequate dark-to-light ratios. This gave him the opportunity to devise a sophisticated mask whose shape gave the required square-wave photocell output.



4 Rebuilt tape pulley system with bedstead frames

This design was the double-meniscus form seen on the Colossus mask preserved in the Science Museum. Dr. Lynch also incorporated small lenses behind each mask aperture, to concentrate the light onto the most sensitive part of the photocells.

The paper-tape feed mechanism had to be very smooth running and stable because of the magnification required. The design used large 9 in (22.5 cm)-diameter aluminium pulleys with the tape looped over a smaller motor-driven pulley to provide a friction drive. There was some anxiety about the strength of paper tape, but it proved to be quite adequate for long continuous running. At 5000 characters per second a tape would last a few days, long enough to achieve a result. In a speed test, Dr. Flowers ran the tape motor at the equivalent of 9600 char-

acters per second, at which speed the tape broke and pieces were hurtled in all directions at nearly 100 km/h!

Colossus in operation

Once a good tape had been acquired it was joined into a loop and then loaded onto the Colossus tape frames, called bedsteads (Figs. 3,4). The tape, which could be up to 40 ft (13 m) long, was threaded round the pulleys. Some pulleys had three grooves round the circumference to accommodate multiple loops. One pulley was on a sliding bracket and could be positioned to take up the slack and get the tension just right.

The Colossus operators came from the Women's Royal Naval Service (WRNS, or 'Wrens'). While one Wren was setting up the tape, another would be plugging in the wheel patterns that the codebreakers

I was given access to what little written information exists

wished to try against this particular intercepted tape.

The codebreaker would then specify the comparison strategies to be followed, and these would be plugged up on the front panels using telephone jacks and cords. Span counters could be set to cause bad parts of the message to be ignored. Limit counts could also be set not to print out counts below a given value, thus reducing output.

Once the tape had been brought up to full speed, the analysis cycles were started. The counts for each loop round the message tape were printed out on an IBM typewriter for analysis by the codebreaker. It typically required two or three days' continuous analysis before the wheel start positions could be determined.

The fate of Colossus

At the end of the war in 1945, all but two of the machines were stripped down to component level. The standard GPO parts for the stripped down machines were returned to GPO stores, while all other parts were literally smashed up – reportedly at Winston Churchill's express command, requiring that all equipment used in producing Ultra (the intelligence output from Bletchley Park) should be reduced to nothing larger than a human hand. The two Colossus machines that survived were dismantled and moved to Eastcote in Ruislip, London. It is thought that the last one was finally decommissioned in 1958 or 1960.

All the construction drawings were finally burnt in 1960. The only surviving records of Colossus were then a number of circuit diagrams, kept quite unofficially by some engineers, and the set of official photographs, taken probably in 1945 in H Block in Bletchley Park.

The resurrectionist

This then was the historical background to Colossus. My problem was to decide whether it was possible to rebuild it.

My early career in valve electronics, followed by time in intelligence, computing and finally in computer restoration at the Science Museum, made me an ideal candidate to rebuild Colossus. By November 1993, I had started work in earnest.

The feasibility of building a replica depended mainly on three factors: per-

mission to build, access to structural and circuit information, and adequate supplies of original components. Because of the secrecy surrounding Colossus, I thought it wise to go through official channels for permission to build. I renewed my old connections with GCHQ, and eventually obtained the necessary clearance for permission to build. One caveat was that the general public would not be allowed direct hands-on access to the replica.

I was given access to what little written information exists, some of which is still classified, and was also allowed to talk to the original designers, builders, maintenance engineers and operators. Information was collected from photographs, drawings, notes and interviews, and collated into computer-aided design drawings, mainly derived painstakingly from the photographs.

The complete rack assemblies and most of the chassis layouts were completed by early 1994. This was followed by the 'bedstead', which held the paper tape, together with the details of the optical system. Some of the control circuits have yet to be defined, but by August 1994, enough information was available to allow construction to begin.

A crucial factor in assessing the feasibility of rebuilding was the availability of contemporary components. The breakthrough came with the discovery of a hoard of over 350 t of Second World War equipment and components in the collection of the Museum Trust of Communications & Electronics in Bristol, some of which it has kindly made available to the project.

An ever increasing net of ex-GPO engineers has revealed large quantities of ex-GPO equipment, which, in many cases, has remained unchanged over 50 years and can be used in the rebuilding. Scouring wireless swap meets and jumble sales also brought in more components. Shaking various 'trees' brought to light important components, including original photocells and lenses.

The information gathered has also allowed the identification of components that will have to be re-manufactured. One of these is a five-pin surface-mounting valve base used for the gas-filled thyr-

trons. 600 of these will be required, but we have a GPO drawing that gives all the dimensions required.

Progress to date

Construction has commenced under the Colossus Rebuild Project in a room in H Block in Bletchley Park. This room originally housed a Mark 3 Colossus, and is thus very appropriate. It has been made available by the Bletchley Park Trust, which is now on course to acquire Bletchley Park as a museum campus in April 1995. I am also museums director to the Bletchley Park Trust, and have created the initial museum provisions, which were opened by HRH the Duke of Kent in July 1994, when he officially inaugurated the Colossus Rebuild Project.

The paper-tape-read system is now completely recreated and built. In this Dr. Lynch was a great help; although well into his 80s, he kindly came to my house in Bedford. We spent a stimulating afternoon in front of my CAD system, reverse engineering his original design.

The 9 in pulley wheels have been cast in aluminium and machined by Chris Burton, a Computer Conservation Society colleague. Much painting, cutting and drilling work was required in constructing the completed paper-tape read system. A large chassis carries the 40 valves required in the amplifiers. This is the only chassis with through-chassis valve bases, so it was back to 1940s chassis bashing with Q Max cutters for me. I remembered the pain well.

The results exceeded my best expectations. The tape pulley system (Fig. 4) is as smooth as silk, delivering a remarkably stable image to the eight original photocells that I have acquired. They all work and deliver the same output as the original notes indicated. The final pulse outputs from the paper-tape system are now exactly as originally specified with the tape running at a comfortable 5000 characters per second.

An interesting point came to light in the final testing of the read system. I was having considerable trouble with changing average signal levels between different test patterns punched onto the paper tape, and eventually traced this to the mask design allowing light through, even when adjacent hole images were (supposedly) off the mask.

**I had no
alternative but
to press forward
as fast
as possible**

I decided that, faced with this problem, I would have designed the mask differently, concentrating on the dark interval between spots rather than the transmitted light on an aligned spot. This led to a double concave form, which is now incorporated and works very well.

When I told one of the original engineers that I had been having trouble with the mask, he immediately remarked that they had trouble too, and the mask that he remembered was like mine, rather than that originally designed by Dr. Lynch. This is one discovery that would never have come to light without the actual rebuild.

In parallel with this work, I have built a replica (on a breadboard, of course) of the original bi-quinary counter, using original valve bases and valves, but cheating with the 1 M Ω resistors, where I used modern components. This worked first time, and actually runs up to 12 kHz, slightly higher than the original spec-

ification. In April 1994 I showed it to Dr. Flowers, who was most impressed. Just seeing it working brought back a lot of memories of Colossus that he thought he had forgotten.

The next stage is to assemble four of the bi-quinary counters on plates, and to bolt them onto the racks that are now assembled. This will allow the control logic to be worked out, and data hole counts to be made from the test tapes on the bedstead. We will then finally be in a position to test whether my faith in the quality of the tape reader is justified.

The future

The next phase of construction depends on getting sponsorship for the project. To date, I have financed everything myself, but am now running out of

money. I felt that, because of the age of the original people involved, I had no alternative but to press forward as fast as possible if I was to have any chance of success.

Bletchley Park is now open to the public every other weekend, the next weekend being 24-25 March. The wartime buildings, an exhibition of codebreaking, and various German cipher machines, including a Lorenz, are on display, together, of course, with the rebuilding of Colossus.

References

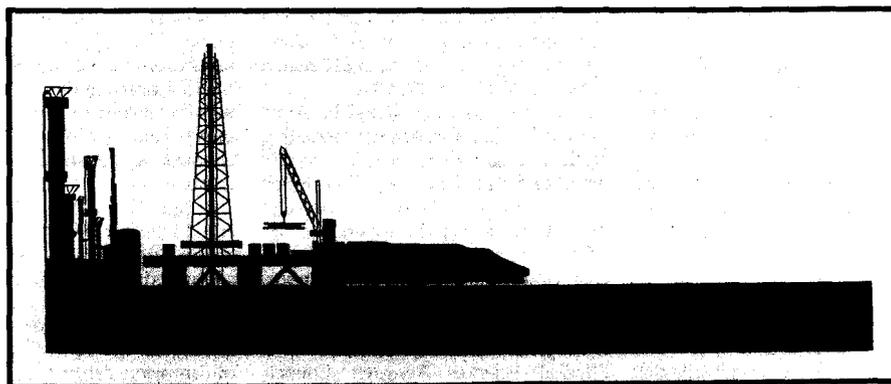
- 1 Randell, B.: 'The Colossus', University of Newcastle upon Tyne, Technical Report Ser. 90, June 1976
- 2 Good, I.J.: 'Enigma and Fish' in Hinsley, F.H., and Stripp, A. (Eds.): 'Code breakers' (Oxford University Press, 1993)
- 3 Flowers, T. H.: 'The design of Colossus', *Annals of the History of Computing*, 1983, 5, (3), p. 239

1st
UK Government
accredited safety critical
software testing services

SAFETY AND INTEGRITY

Testing and Certification for Safety Critical Software and Systems

ERA
TECHNOLOGY



A Service in Trust, Competence and Quality.

ERA Technology - the first to offer UK Government (NAMAS) accredited safety critical software testing

- Integration with general electronic system assessment
- Objective & repeatable safety critical s/w testing
- Testing to draft IEC and other standards
- Services backed by a broad engineering capability
- Cost-effective test & assessment services
- Certificate of product test

Enter 011

Telephone: +44 (0)1372 367080. Fax: +44 (0)1372 367099



Please supply more information on Safety Critical Software

Name _____
Company _____
Address _____

To: Kathryn Tame
ERA Technology, Chevee Rd.
Leathhead, KT22 7SA
England