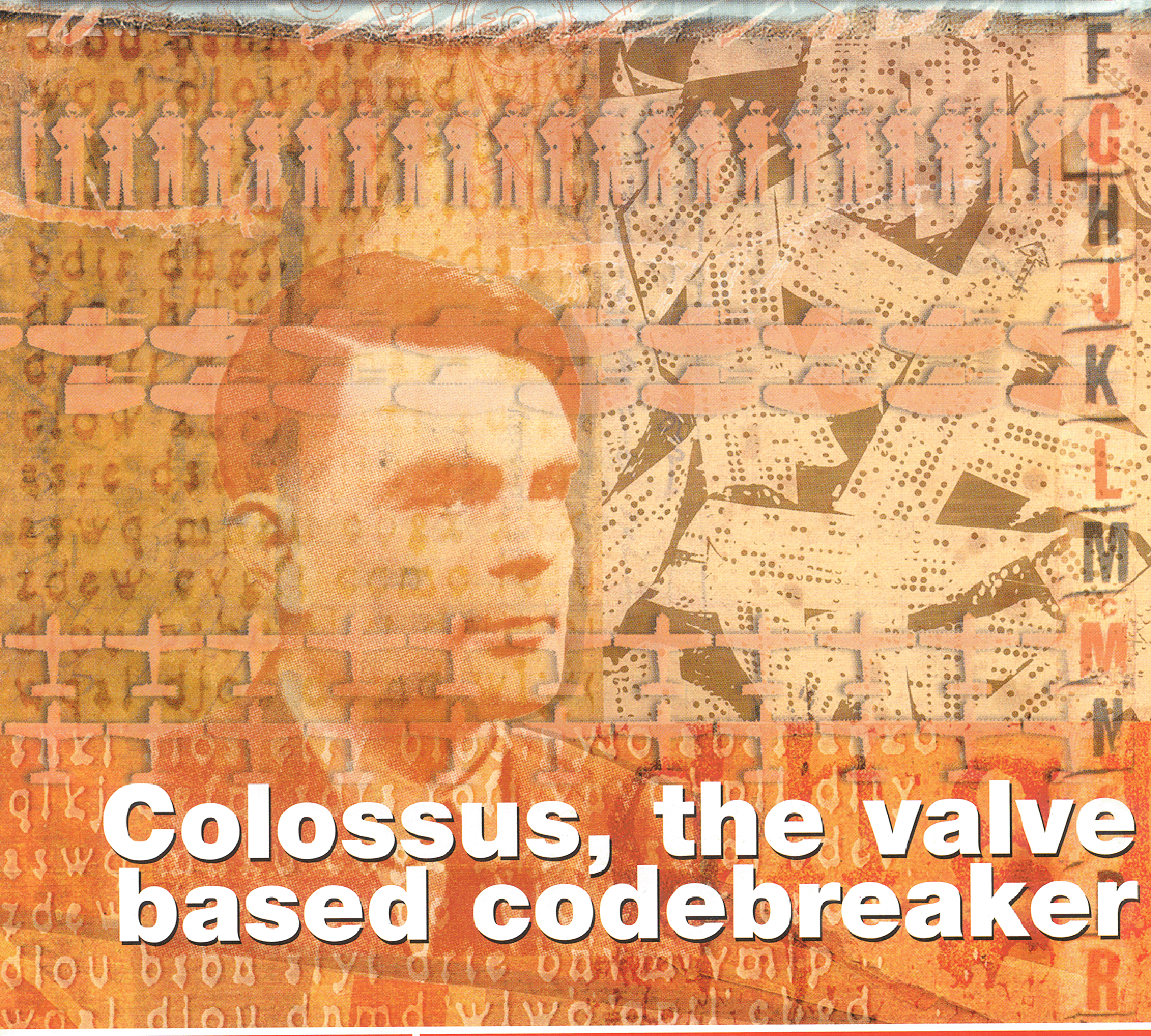
SEARCHING FOR SUPPLIERS? GO TO WWW.DESIGNSELECTOR.CO.UK

Tuesday 9 January 2001

New Electronics

CONNECTING ENGINEERS WITH TECHNOLOGY - www.neon.co.uk



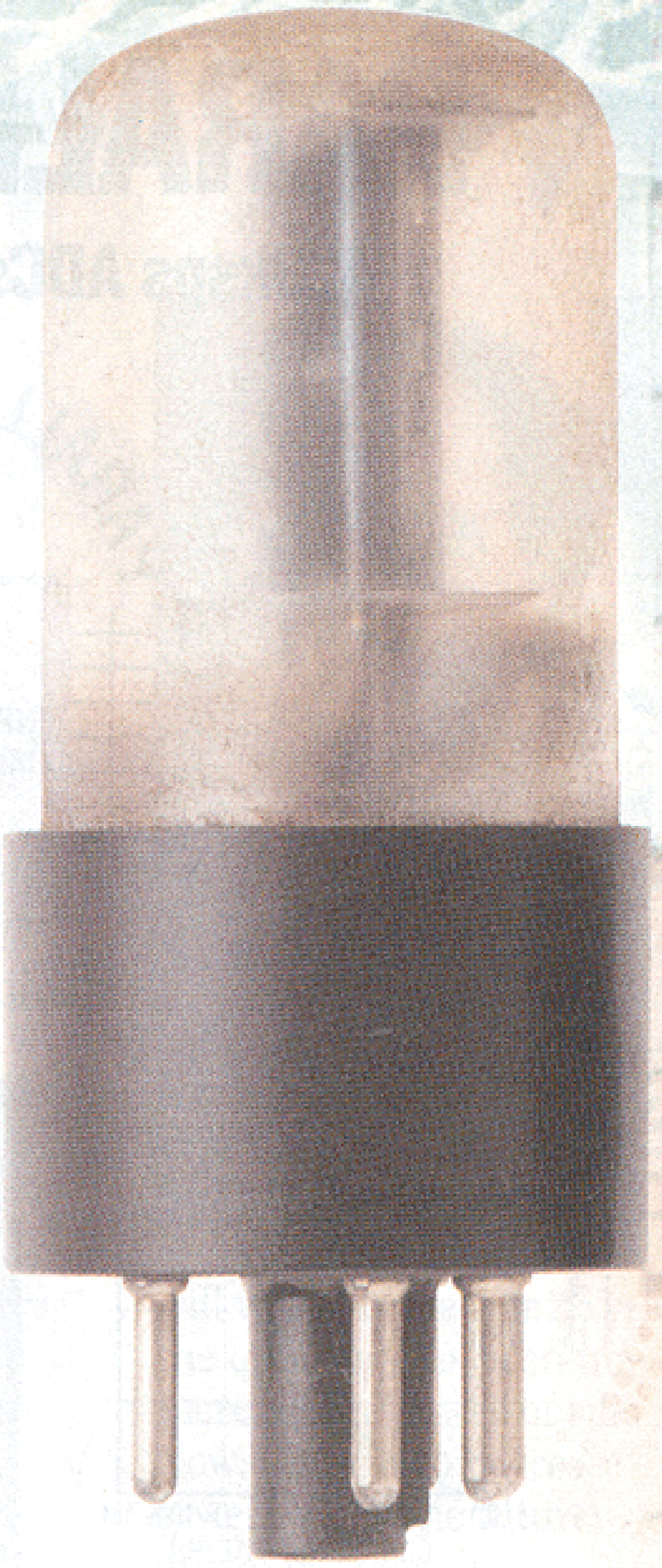
Colossus, the valve based codebreaker

SPECIAL REPORT: IC FABRICATION

EMBEDDED INTERNET BREEDS A NEW TYPE OF WEB BROWSER
CORES ARE BECOMING SOC'S FLEXIBLE FRIEND
CURRENT BLOCKING IN PORTABLE APPLICATIONS
TEAMWORKING MEANS NO WALLS, NO PCB REWORK

Valves crack codes

The world's first electronic computer, used for code breaking during the second world war, has been reconstructed. *By Louise Joselyn.*



Bletchley Park, the famous wartime home of Allied code breaking, is also the location of Colossus, the world's first electronic computer. You may have thought that honour belonged to US machine ENIAC, switched on in 1946. But Colossus, designed and built in the UK, was developed during 1943 and in use from January 1944. By the end of the war, 10 systems were operational at Bletchley Park. However, soon after, eight of the ten were dismantled. Two went to Eastcote in North London and then to GCHQ at Cheltenham. The last two were dismantled in about 1960.

Colossus' very existence was secret until the 1970s, when information began to emerge. The US had been mistakenly claiming it had developed the world's first large scale electronic digital calculator for some time. Until four years ago, it could claim ENIAC was the oldest in operation. However, a successfully rebuilt Colossus changed that in a move somewhat cheekily timed to coincide with the 50th anniversary of ENIAC's inauguration.

It wasn't until 1993 that Tony Sale, now curator of the Bletchley Park museum, set himself the challenge of rebuilding Colossus. Sale, who was working at the Science Museum restoring some early British computers, began gathering the available information. "This amounted to eight 1945 wartime photographs plus some fragments of circuit diagrams which a few engineers had kept; quite illegally, as engineers always do!"

Ironically, the most valuable data on Colossus came from the US. In 1995, the US National Security Agency (the equivalent of GCHQ) released 5000 World War II documents into the US National Archive. Sale quickly trawled the list. "I was amazed to see documents relating to UK encryption efforts." Copies revealed these documents were written by American servicemen seconded to Bletchley Park when the US entered the war. "The most important one, written by Albert Small, is a complete description of Colossus code breaking." This report enabled Sale and his team to work out the function of about 90% of the circuits and program switches on Colossus.

Colossus, like ENIAC, is a hard wired and switch programmed machine, rather than a stored program computer. Its parallel nature, despite predating integrated circuits of any kind, makes it fast, even by today's standards. In fact, Colossus is as fast as a modern Pentium based pc programmed to perform the same code breaking task!

Parallel processing

Colossus, designed by Dr Tommy Flowers, uses an array of 1500 valves to speed decryption of intercepted messages (see box). The machine lives up to its name: Colossus occupies a large room and comprises eight racks, each 2.3m high, arranged in two bays about 5.5m long. The paper tape reader and tape handler – known as the bedstead – are supplied as extras! The front bay of racks is 1.6m from the rear bay. The key components are: optical reader; master control panel; 501 thyratron rings and related driver circuits; optical data staticisors and delta calculators; shift registers, logic gates, counters and their control circuits; span counters; relay buffer store and printer logic. The power packs comprise 50V Westat units stacked in series to give +200V to –150V. Total power consumption is about 5kW, most of which powers the valve heaters.

Advanced technology

The intercepted message, punched onto ordinary teleprinter paper tape, is read at 5000 character/s. The sprocket holes down the middle of the tape (which is joined to form a loop) are read to form the clock for the whole machine. This avoids any synchronisation problems. The speed of the tape, therefore, defines the speed of Colossus.

Although it could have run faster, 5000cps was deemed safe. At this speed, the interval between sprocket holes is 200us, during which time Colossus could perform 100 Boolean calculations on each of the five tape channels and across a five character matrix. The gate delay time is 1.2us, which Sale reminds us 'is quite remarkable for very ordinary valves'.

The broad principle of Colossus is to count, throughout the length of the text, the number of times that a Boolean function between the text and the generated wheel patterns has either a true or false result. At the end of the text, the result is passed to relays before being printed on a typewriter during the next pass of the text. Effectively, this is an early form of double buffering.

Colossus has two operational cycles. The first is controlled by the optical reading of the sprocket holes. The optical reader system of 1942 is based on hard vacuum photocells. Six photocells, originally developed for proximity fuses in anti aircraft shells, are used to enlarge the image of the paper tape tenfold. The output from the data channels goes to the staticiser and delta circuits, where it is sampled on the back edge of the standardised sprocket pulse, as are the outputs from the rings of thyratrons representing the Lorenz wheel patterns. The result of the logical calculation is sampled on the leading edge for input into the counter circuits.

The second cycle begins with the electrical signal from the photocell reading the stop hole on the tape. This stop pulse sets a bistable circuit which stays set until the optical signal from the start hole is read, typically about 100ms. Any settings on the relays from the previous count are released before the new count is read to the relays. Then the counters and the thyratron rings are cleared and the thyratron rings strike the next start point. When the bistable is reset by the start pulse, sprocket pulses are 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.

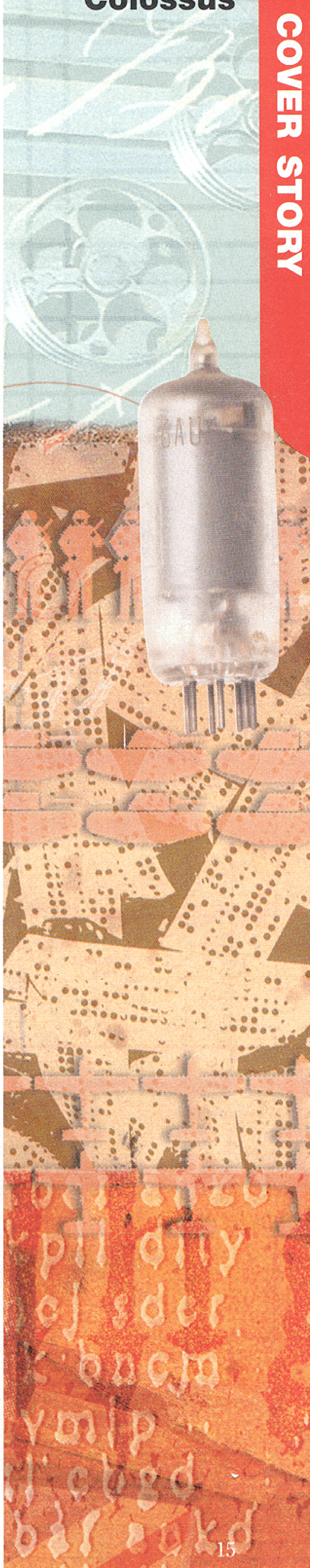
Tape reader

Colossus' optical tape reader uses a bright light shone through the tape and focused onto hard vacuum photocells, one for each bit of data and one for the clock pulse. Before the light hits the photocells, it is 'shaped' by passing through an optical mask, which helps ensure the signals produced by the valves are uniformly square.

The rebuilt Colossus at Bletchley is housed in a room with windows at one end for public viewing. To improve visitor visibility, it was decided to capture the signals from the photocells via an oscilloscope and display them on a large colour screen.

When the technical team at virtual instruments company Pico volunteered to help display the signals, the task was thought to be simple. The instruments were regularly connected to computers with clock speeds thousands of times faster than Colossus. In fact, it proved a challenge! The original idea was to place a pc and ADC-212 'scope in the public viewing area and run the analogue signal from the valves along a long cable to the 'scope's inputs. The problem was that the extra capacitance from the leads prevented the valves from operating correctly. To solve this problem Pico technician David Sabine built a high input impedance, low capacitance buffer amplifier.

The cables are taken up through the roof void, across and down to the computer with the pc based 'scope. When connected, the system worked first time.



The thyratrons used on Colossus are gas filled triodes which strike a discharge arc between anode and cathode when the grid voltage is raised to allow electrons to flow. When struck, this discharge continues independently of the grid voltage, allowing the thyratron to act 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. A shift register is constructed when one thyratron strikes the next in the ring and 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 staticisors and delta 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 ±80V. A one clock pulse delay 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, that is 1, when current data is different from previous, and 0 when current equals previous. Up to five shift elements can be cascaded, giving a 5bit shift register.

Programming of the cross correlation algorithm is achieved by a combination of telephone jack plugs, cords and switches. The changeover from direct to delta could also be achieved by switches.

The circuit layout is surface mounted components (proving the old adage that 'what goes around comes around!') on metal plates bolted to the racks. The valve holders are surface mounted with tag strips for the components. Sale points out: "This form of construction has much to commend it. Firstly, both sides of a rack can be used. Secondly, wiring and maintenance are easy. Lastly, cooling of the valves is expedited by them being horizontal."

Right first time

Unlike some of today's complex electronic products, Colossus was successful on its first test against a real enciphered message tape. It was a highly valued feat of engineering: it reduced the time to break Lorenz messages from weeks to hours. It provided vital information to Eisenhower and Montgomery prior to D-Day. By the end of hostilities, 63million characters of high grade German messages had been decrypted.

Today, Colossus can be seen at the Bletchley Park Museum. For more information see www.bletchleypark.org

Lorenz ciphers

In order to communicate by radio in complete secrecy, the German Army High Command used the Lorenz cipher machine, based on Vernam's additive method for enciphering teleprinter messages. Teleprinters are not based on the 26 letter alphabet, but the 32 symbol Baudot code. The Baudot code output consists of five channels, each of which is a stream of bits which can be represented as no hole or hole, 0 or 1, dot or cross.

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.

The obscuring characters were added using modulo-2 addition, which works in the same way as the XOR operation in logic. The same obscuring characters, also generated by modulo-2 addition, applied to the received enciphered characters, cancel the obscuring characters and leave the original message.

Vernam proposed the obscuring characters should be completely random and such a cipher system is unbreakable. In application, however, the difficulty was how to ensure the same random character tapes were available at each end of a link and that both were set to the same start position. The Lorenz company decided it would be easier to construct a machine to generate the obscuring character sequence. By default, this was pseudorandom and potentially breakable.

Teleprinter signals being transmitted by the Germans in early 1940 were identified as being enciphered using Lorenz in the Vernam manner. Little headway had been made into breaking the cipher until the Germans made one horrendous mistake in August 1941. An operator had to resend a 4000 character message and used the same obscuring character string by resetting the Lorenz machine to the same start position. Keying differences between the messages overlaid with an identical obscuring sequence allowed the code breakers to recover both texts, and a long stretch of the obscuring character sequence. From this, came the logical structure of the cipher machine.

Early in 1942 the Post Office Research Labs at Dollis Hill began producing an implementation of the logic using a rack of uniselectors and relays. It was a breakthrough, but manual code breakers still had to work laboriously for four to six weeks to crack the settings used for a particular message.

The mathematician Max Newman began to automate the process for finding the settings used for each message. However, the mechanical system of two punched paper tape wheels was difficult to keep synchronised at 1000 characters/s. Colossus was the solution: the wheel patterns were generated electronically in ring circuits, doing away with one paper tape and eliminating the synchronisation problem.