The Colossus

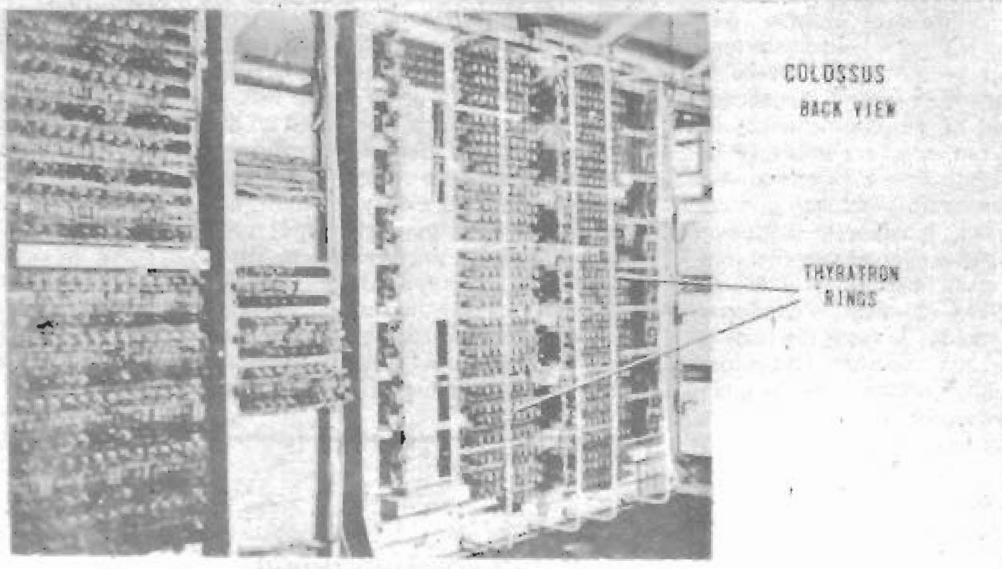

FIG. 3

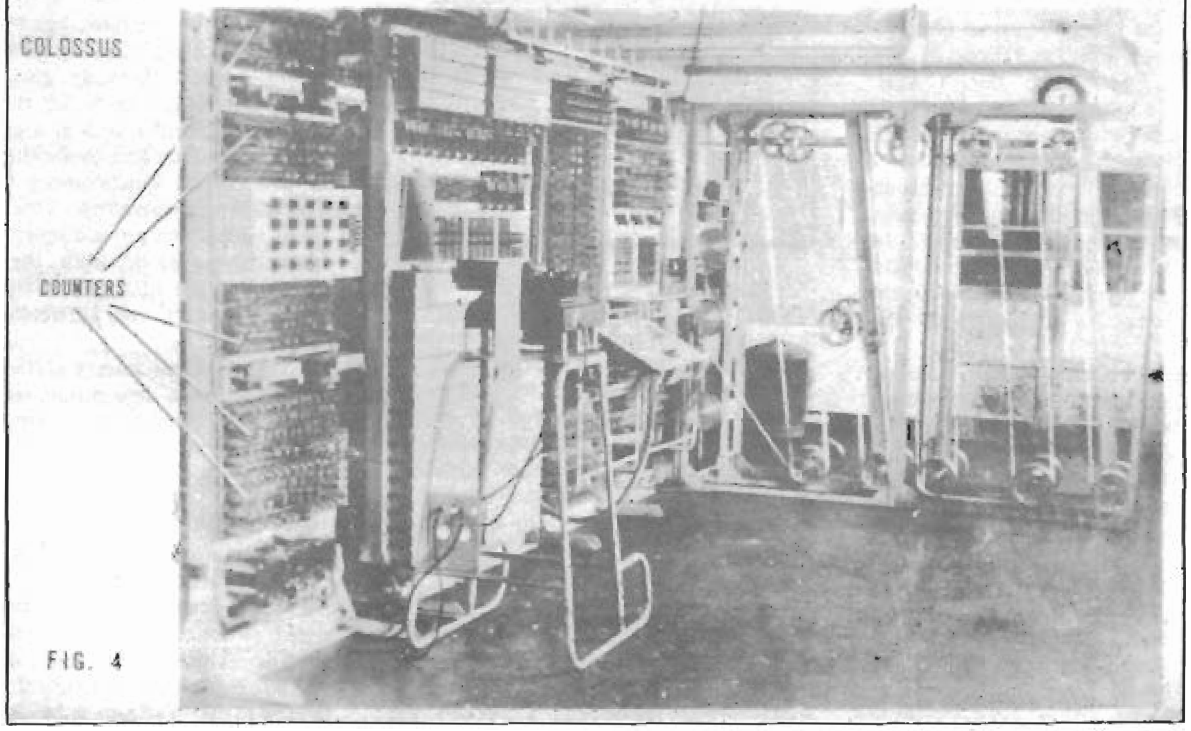

FIG. 4

Thirty years after the fact, the British reveal to the world that it was they, and not the Americans, who invented the first practical electronic computer. Roger Allan lets us in on the secret.

THE LIFTING of the British Official Secrets Act after it had run its customary thirty years has resulted in an absolute mother lode of detail and information concerning the wartime allies' *modus operandi*. So great is the volume of data now available, that virtually all general histories of the Second World War published before 1975 have been rendered redundant. Historians, utilizing their customary care, are slowly sifting through the mountain of information available, and while their work is far from complete (in fact, most of the documents haven't even been read yet), a number of interesting elements have come to light that touch on some rather peculiar subjects, including, odd as it may seem, computers — or more specifically, the very first computer, moreover, one which not only preceded ENIAC (customarily considered in all the textbooks as being the first) by several years, but one which had a computational ability not matched by mainframes for over a decade, capable as it was of working at some 25,000 logic decisions a second.

The history of the German *Enigma* machine and how it produced a seemingly unbreakable code is fairly well known — including how the Canadian, William Stephenson, and his colleagues at Bletchley Park, north of London, broke it (see *Stephenson,* ETI, Sept. 1982). Their methods of decipherment were slow even when the code was broken, and as the codes (dependent on the positions of a number of rotors internal to the transmitting machine) were changed regularly, sometimes as often as once a day, the decipherment of the new code produced by the machine produced great gaps in the available intelligence derived from this source.

Further, the Germans had a second machine known as the *Geheimschreiber* or 'secret writing machine'. Unlike *Enigma,* which was used by front line commanders as well as for communications to and from headquarters, the *Fish,* as it was known to the British, was only used by the upper echelons of the German High Command — Hitler using it for overall strategic directives, the Ministry of Foreign Affairs for communicating with neutral embassies, and so on.

When the British broke the *Geheimschreiber* code has not yet been determined (it is still buried in the pile of currently unread data at the Public Record Office, Britain's national archives, in London), but most probably it was late in 1941. Decipherment was slow and by hand, and as the code was changed on a daily basis, most often the decipherment, when it was completed (which was rare), was completed weeks or even months after it was sent. The machine, more complicated than the *Enigma,* worked on ten rotors, each one of which could be set differently. This produced a code of several billion possibilities, rather a long job to sort out by hand, even when utilizing Boolean algebra. It had the great advantage in that it automatically enciphered a signal typed on it in clear and sent it to the telegraph or radio station at the rate of sixty-two words a minute, without the need for a cipher clerk (which was one of *Enigma's* great weaknesses). In order to receive the message a similar machine was needed, which automatically typed out the text. It was in essence a teleprinter, based on the telegraph code of Baudot and Murray. This code contained thirty-two separate elements embracing twenty-six letters, ten numbers, punctuation, teleprinter functions, line feed, carriage return, letter spacing and letter and number shift. In order to fit all this into thirty-two elements, the code had to be used twice over; in a lower case for letters and in an upper case for numbers and punctuation.

"... a computational ability not matched by mainframes for over a decade ..."

In early 1942, Bletchley Park was a hodgepodge of interesting characters — mathematicians rubbing shoulders with archeologists, front line battle weary officers chatting with physicists, and so on. It was from this compendium of diverse sorts, producing a marvelous cross-fertilization of ideas, that the major British intelligence operations were determined and built, where the *Enigma* codes were cracked, for instance.

Not a ZX-81 Yet . . .

In early 1942 a Cambridge mathematician, M.H.A. Newman, joined the staff, and it occurred to him that perhaps it would be possible to build a machine that would automatically and very quickly do the sorting and comparison work currently done by hand, but would do it much more quickly. He persuaded the Powers That Be to act on his idea, and a section was set up under his direction, known as the "Newmanry", in Hut F at Bletchley Park. Under his direction, a team of mathematicians, with the assistance of several engineers from the British Post Office Research Station at Dollis Hill, built a machine. It used 80 valves, and stood in two general-issue Post Office equipment racks about 8 feet high. It utilized a photo-electric reader and could scan 2000 telegraph characters a second.

Its operation was quite straightforward. Five unit Murray Code elements were punched onto a paper tape, containing the German cipher, which was fed into one of the two readers. The tape was joined to form a large loop which ran continuously over a system of pullies past photoelectric cells. A key tape, smaller in length than the first tape and containing the deciphering telegraph units, was fed into the second reader. Telegraph tape, like old style computer tape, had sprocket holes in it. As the sprockets rotated, they drove the two tapes. As one tape, the key tape, was shorter than the first tape by one character, every revolution of the tape produced a different key unit passing through the reader against the message units. Named the "Heath Robinson" after the constructor of crazy machines, it essentially depended on a statistical system of breaking codes. It could operate at two thousand characters a second — that is, when it worked, which it frequently didn't, as the tapes kept breaking.

As Odette Wylie, a WRNS who worked on the machine, has been quoted as recalling, "It was a long time before we found some sufficiently gluey material that would stand up under the strain of going round and round at a great speed. The fact that we had to get the two tapes to run exactly synchronized was also a very difficult operation. When they did break, it was not just a question of breaking and lying on the floor, they flew into the air and got entangled in the machine, in little corners, very difficult to get out again."

Further, the binary system counting procedure was inaccurate, due to the unreliable relays, and the single loop of tape which provided the key was inadequate.

Invention

It was about this time, January 1943, that two Post Office engineers, T.H. Flowers and S.W. Broadhurst, specialists in high-speed switching, joined Bletchley Park. Familiar with Alan Turing's 1936 paper on the creation of an artificial brain, and realizing that vacuum tubes had a very high degree of reliability if kept in constant operation (rather than being switched on and off), they suggested the building of a "Super Heath Robinson." After some opposition, the Powers That Be gave the go-ahead, and the first computer, the Colossus Mk I, was built. Design commenced in Februrary 1943, and was delivered in working order in December of the same year.

Based on some 1500 valves, the major difference to the "Heath Robinson" was that the key tapes were replaced by electronically-generated keys. The ten *Geheimschreiber* rotors were simulated by ten rings of thyratron triode valves, which, containing argon gas, acted as very high speed switches and were capable of passing high current. One valve in a particular ring was conducting at any given moment, when its neighbour would take over, thus simulating the passage of the loop continuously through the photo-electric readers.

The interface between the machine and the operating cryptoanalyst was via a bank of switches, whereby the cryptoanalyst would ask the machine to make certain adjustments to the cipher keys. She would be sitting in front of an electric typewriter looking for the tell-tale letter recurrence which would indicate a gradual solving of the cipher text. Once the code was broken, it could reproduce the results *ad infinitum* for all further traffic using that code — to the extent of 10^{11} consecutive elementary Boolean (and/or) equations without error.

It was therefore the first electric computer, and the first statistical brain containing a memory which did not make mistakes.

Similar to the *Enigma* machine, the *Geheimschreiber* was constantly being improved, and during the war there appeared five versions (models 52AB, 52C and others). One of the modifications consisted of some of the rotors rotating irregularly, being driven by prawles, retaining an eccentricity. The Colossus Mk I was unable to handle this eccentricity. As such, an improved version, the Colossus Mk II, was designed to deal with this modification to the German *Fish*.

IF Unbroken THEN Keep Trying

The function built into Colossus Mk II to solve the eccentric rotors was Conditional (branching) IF logic — it could make decisions. While this is fundamental to modern computers, this machine was the first to use it. It utilized 2500 valves, and its reader could scan 5000 characters a second. Five such readers could be placed in parallel, giving it an overall operating speed of 25,000 characters a second — a speed not duplicated by other computers for over a decade. Output was fifteen characters a second on an electric line printer.

The speed at which this machine was designed and built is quite extraordinary. The go-ahead was given in March of 1944, with a delivery date by D-Day, June 6. The first of ten Colossus Mk IIs was delivered on June 1.

As to what the twenty cryptoanalysists, twenty engineers and 250 WRNS operators at Bletchley Park attached to the "Newmanry" deciphered on the Colossus has as yet not been determined, other than that it was used for the *Ultra* intelligence, never on *Enigma* messages.

The story of what happened to them after the war is simply told. They were dismantled, and sold in unidentified lots to the surplus stores, along with the other electronic bits and pieces from Bletchley Park. ETI