Thomas H. (Tommy) Flowers

Builder of Colossus, the cryptanalytical machine designed by Alan Turing and others at Bletchley Park, England, perhaps the first electronic computer in the UK.

Education: BSc, London University, 1933; Honorary DSc, University of Newcastle upon Tyne, 1977.

Professional Experience: Post Office Communications Laboratories, 1930-1950; ITT-England, 1950-1970.

For its time Colossus was a notable innovation, different from its predecessors in many dramatic aspects. Flowers made the following claims for Colossus:

1. It was electronic. Other machines, such as Heath Robinson, had had electronic subsystems, but they were of minor size. Colossus had 2,400 vacuum tubes-big bottles. Ah, the warmth at 2 a.m. on a damp, cold English winter!

2. It was digital, and experience with digital circuits was then very limited. The vacuum tubes of the day were mainly intended as amplifiers; manufacturers strove for linear response. Fortunately for Colossus they were successful over only a limited range.

3. It was programmable by means of a switchboard. Toggle switches enabled one to choose among binary functions of the input, which was a long string of cipher text, and then the outputs of these functions were counted. At the end of each pass of the input string, the counts were used to control the printer, suppressing those counts of lesser interest.

Colossus was not sequence-controlled, nor was its program stored. Nor did any of us see that possibility.

Parameters of the cipher were entered by means of the bottle plugs on the remote back of Colossus-to keep leads short. The cipher text was on very long Teletype punched tapes pasted into a loop and then run at 5,000 characters per second. When a paper tape parted it caused some excitement.

The tapes were prepared and mounted by women of the Women's Royal Naval Service (WRNS)-called “Wrens”--who were very skilled and adroit. Others tried but invariably caused trouble. Without the Wrens they were helpless.

Colossus was useful in more than one way, and there were even demonstrations applying it to number theory. But these demonstrations were more notable for their ingenuity than their effectiveness.

A successful result from Colossus was not plaintext, but an intermediate product that was completed by hand by skillful specialists.

The cipher system under attack was on-line, an integral part of the communications links; a typist at one end ran a typewriter at the other. Once synchronization had been established, the typist fed in message after message until the backlog had been exhausted. A cryptanalytical solution would reveal an avalanche of plaintext.

This cryptanalysis was a superb technical achievement, and the cryptanalysts were very proud of it. At the same time they were painfully aware that their dominance was precarious, and were fearful that a change by the Germans might deprive them of their sustenance. When I was scheduled by the US Navy to join the "Newmanry" as a working member and observer, my plans were unsettled by a dispatch that the Germans had begun to use new wheel patterns each day instead of once a month, and that there was little chance that the system would ever be read again. But two months later the effort had been doubled and redoubled, and more was being read than ever before. Part of the redoubling was to build more Colossi; earlier there had been one, now there were to be twelve.[1]

BIBLIOGRAPHY

Biographical

Flowers, Thomas H., "The Design of Colossus," *Ann. Hist. Comp., Vol.* 5, No. 3, July 1983, pp. 239-252.

Lavington, Simon, *Early British Computers,* Digital Press, Bedford, Mass., 1980. See Chapter 5: "The ACE, The "British National Computer."

Randell, Brian, "The Colossus," in Metropolis, N., J. Howlett, and Gian-Carlo Rota, *A History of Computing in the Twentieth Century,* Academic Press, New York, 1980, pp. 47-92.

UPDATES

Tommy Harold flowers died October 28, 1998. Portrait added. (MRW, 2012)

[1] Campaigne, Howard. From the foreword to Flowers, Thomas H., "The Design of Colossus," Ann. Hist. Comp., Vol. 5, No. 3, July 1983. Howard Campaigne joined the newly formed National Security Agency after the war, where he eventually became chief of research. After serving as professor and chairman of the Mathematics Department at Slippery Rock State College from 1970 to 1976, he retired to Portales, N.M.