THE Transition FROM MECHANISMS TO ELECTRONIC COMPUTERS, 1940 TO 1950

Donald W. Davies, Independent Consultant
15 Hawkewood Road, Sunbury-on-Thames, Middlesex UK, TW16 6HL

Abstract

The peak of mechanical cryptography was reached in World War II, then electronics rapidly replaced these machines. A very remarkable technology then ended. Some of the best examples that I have found will be illustrated. The paper continues with some memories of building the first computer at NPL during 1947 to 1950.

The age of mechanisms

The difference engines and analytical engines designed by Charles Babbage would have been, if completed, one of the greatest achievements of the mechanical age. Computing devices remained mechanical (or electro-mechanical) for another 100 years. Today we are in the electronic age and it is interesting to look at the short period of transition from mechanisms to electronics, which began about 50 years ago. In this paper I shall consider only digital systems and my examples come from cryptography and my own memories of the first electronic computers.

Electronics can be pretty, but what you see is only distantly related to its function. At the peak of the mechanical age, the function of mechanisms was very clear; they could be seen working at human speeds. This led their designers and constructors to emphasize their function with shapes of striking beauty and with surface finishes that were often much more elaborate than strictly required. Not only steam engines and pumps had this quality - it can be seen in Babbage's designs and in his test assemblies.

It has often been assumed that Babbage did not complete his machines because the technology of the time was inadequate. The recently completed difference engine No.2 at the London Science Museum shows that Babbage's machines do work, when they are built with the materials and precision available to Babbage. The design needed
several corrections and some counterbalancing springs. The very complex running carry mechanism works perfectly and spectacularly, and wheels that are not being stepped are firmly held. The only concerns of its designers and operators at the Science Museum are with lubrication and with wear. The part of the machine which impressed the printing plates has not yet been built and urgently needs sponsorship.

Calculating mechanisms often have repeated units such as counter wheels and registers but they cannot be organised simply by linking together large numbers of very simple devices in the way that gates and storage cell are used. The best that can be done is illustrated by Babbage's notation for mechanisms and his suggestions for some general-purpose mechanical principles. Conrad Zuse once described to me a mechanical binary store array with which he had proposed to make a mechanical 'minicomputer'. But these were exceptions and usually a digital mechanism is designed as a whole rather than assembled from identical subunits. In this respect, the precursors of the gates and cells of electronics were electro-mechanical systems such as telephone exchanges which used relays and rotary switches as subunits, and appeared briefly in cryptography.

To illustrate this period of transition I will first describe two cryptographic mechanisms used by Germany in WWII, then some of my own experience with the first electronic computers.

On-line ciphers of World War II

The Enigma machine is very well known. This was operated off-line, producing a written ciphertext which was then manually transmitted. In the Defence Museum in Oslo there are printer attachments for enigma machines, remote displays and a large commutator called 'Enigma-Uhr' which could be wired to the plugboard to give hourly changes of key. Fortunately for the Allies, this last device came into use very late. By upsetting the involution property of the plugboard, the Enigma-Uhr would have given a major problem to the cryptanalysts.

There were two on-line machines in wide use by the German forces.

One was known as SZ40 or SZ42, where SZ stands for Schluessel Zusatz