Colossus and the German Lorenz Cipher – Code Breaking in WW II

Anthony E Sale, Hon. FBCS

Bletchley Park Trust
tsale@qufaro.demon.co.uk

The Lorenz cipher system was used by the German Army High Command in World War II. It used a binary additive method for enciphering teleprinter signals.

The Lorenz machine used 12 wheels each with a mutually prime number of small cams round its periphery, 501 in all. The wheels were geared together to ensure a very long repetition period. The task facing the code breaker was to find the patterns of cams round each wheel and the relative start positions to which the operator had turned the wheels before sending his message.

The cryptographic structure of the Lorenz machine was given away by a catastrophic mistake made by a German operator on 30th August 1941.

A special section was set up in Bletchley Park, the Allies code breaking establishment, to attack this cipher, codename "Fish". Laborious hand methods were worked out which showed that it was possible but only with 4 to 6 weeks delay for deciphering each message.

Professor Max Newman had ideas for automating and speeding up the breaking. In March 1943 he approached Dr Tommy Flowers who started designing and building Colossus to meet Max Newman's requirements for a machine to break Lorenz more quickly. Colossus was working by December 1943 and installed in Bletchley Park over Christmas 1943. It was working by January 1944 and successful in its first trial on a real cipher message. It reduced the time to break Lorenz from weeks to hours providing vital intelligence just in time for D Day, the invasion of Europe on 6th June 1944.

After D Day 10 machines were built and working in Bletchley Park. Then at the end of the War eight machines were totally dismantled, two went to GCHQ at Cheltenham. These were destroyed in 1960 together with all the drawings of Colossus and its very existence was kept secret until the mid 1970's.

In 1991 Tony Sale and two colleagues started the campaign to save Bletchley Park from property developers. At this time he was restoring some early computers at the Science Museum in London. He thought it might be possible to rebuild Colossus and started gathering information. Eight wartime photographs and some fragments of circuit diagrams were recovered. He decided to have a go and had the basic Colossus working by 6th June 1996.

Now four years further on Colossus is nearly completed and demonstrates the power of what is now recognised as the world's first electronic programmable digital computer.