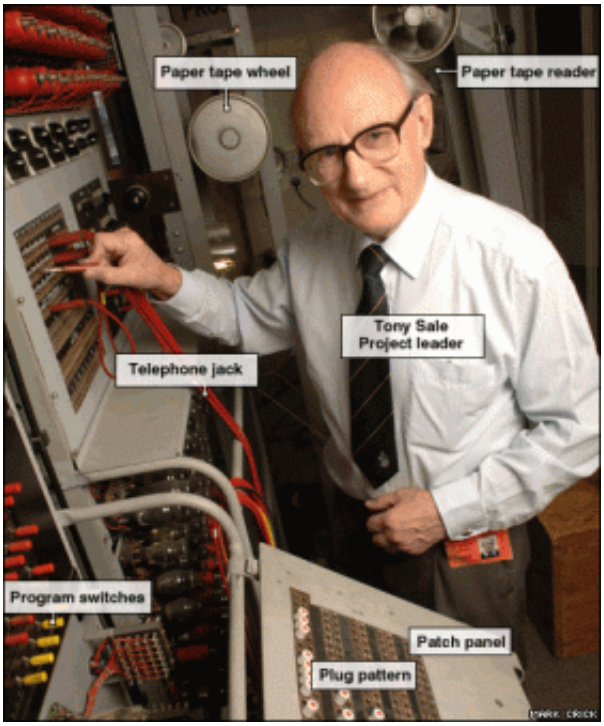
Reconstructed WW II Code Cracker Colossus Defeated

November 16 2007, by Mary Anne Simpson



Colossus & Reconstructor Tony Sales: BBC - How Colossus Works

A monumental achievment in reconstructing Colossus the first code cracker computer used by Allied forces in World War II. In a timed contest between Colossus and the modern PC Colossus was defeated by a modern program and a 1.4 GHz PC.

A fourteen year project to reconstruct the World War II Allied forces

Colossus the first code cracking computer ended in a match defeat against a modern 1.4 Ghz PC. The cipher event was instigated by The British National Museum of Computing and Cryptography at Betchley Park home of the newly reconstructed Colossus Mark II. The event challenged all interested parties to compete with Colossus in the deciphering of three enciphered messages. The German participants sent the messages utilizing the Lorenz SZ42 teleprinter using the same radio protocols as the German high command used in World War II.

The original Colossus is regarded by many to have been instrumental in shortening the war in Europe by as much as 18 months. The Colossus about the size of a British small lorry was capable of deciphering messages sent by Hitler to his generals. The Nazi based Lorenz SZ40/42 machine enciphered messages that were sent by radio to the German high command. The only reason the messages were capable of deciphering was that the Lorenz SZ40 encryption was not entirely random.

The process to unscramble the messages were painstaking and involved several layers of deciphering tasks. First the captured messages sent via the radio were punched on to paper tape. The paper tape was fed into Colossus at the rate of 5,000 characters per second. The inputted data became part of the memory of Colossus. Colossus then analyzed the data to determine the wheels of the Lorenz might have been set up to encipher the message. Various functions of the Colossus were used to perform this statistical analysis. The end result with a little luck thrown in would be a printed tape with the exact wheel of the Lorenz so the message could be deciphered. Generally it took about six hours to decipher a message.

After World War II the six known Colossus computers were broken up and destroyed for a variety of reasons. Some 14 years ago Tony Sales and the founders of the aspiring British National Museum of Computing

and Cryptography embarked on the project to reconstruct a Colossus using photos and scant information about the original machine.

The winner of the cipher event Bonn, Germany resident Joachim Schuth used a program he wrote in ADA programming language to decipher the coded messages. The very noisy transmission was received by Schuth yesterday and his 1.4 Ghz PC took only 46 seconds to decipher the message using his program. The total time involved was two hours from the time when the message was first received to the end when it was actually deciphered.

Unfortunately the radio transmission was troublesome due to atmospheric conditions. The Colossus got off to a rough start by getting the message late yesterday and beginning the process of deciphering early this morning when it was announced by Heise a German news service that Mr. Schuth had all ready cracked the code.