Enigma code-breaking machine rebuilt at Cambridge

13 July 2020

Credit: University of Cambridge

Cambridge Engineering alumnus Hal Evans has built a fully-functioning replica of a 1930s Polish cyclometer—an electromechanical cryptologic device that was designed to assist in the decryption of German Enigma ciphertext. The replica currently resides in King's College, Cambridge.

Work on the hardware-based replica began in 2018, as part of Hal's fourth year Master's project under the supervision of King's College Fellow and Senior Tutor Dr. Tim Flack. The aim was to investigate further into cryptologist Marian Rejewski's cyclometer—an early forerunner to Cambridge University mathematician Alan Turing's machine, known as the Bombe, which was used to crack the German Enigma code during the Second World War.

Hal said he chose to work on the cyclometer as it was the very first machine used to assist the decryption effort. To his knowledge, the replica is the first fully-functioning hardware-based electromechanical cyclometer to exist since the years preceding the Second World War. The original machines would have been destroyed in 1939 to prevent them from falling into the hands of German invaders.

"Due to the cost and the mechanical complexity of reproducing the original machine, other efforts to create a replica have been software-based to date," said Hal. "This presented an opportunity to recreate an important fragment of history. It has been a privilege to work on such a unique project which is a fascinating combination of Engineering, History and Mathematics. The replica took just over a year to complete, with generous funding from King's College, which saw the obvious link with the work of one of its most famous alumni, Alan Turing.

"The successes at Bletchley Park are well known in the UK and, while the Polish contribution is certainly acknowledged, I think its exact extent and significance are not widely recognised. Researching into Rejewski and his colleagues, I wanted to discover more about their efforts, and the more I looked, the more interesting the story became—quite how advanced the Poles were in their understanding of Enigma compared to the British in 1939 is remarkable. The Poles were, in fact, the first to crack the Enigma code prior to the start of the War, using various systems, complicated high-level mathematical methods and purpose-built machines. Their work and knowledge proved invaluable, and laid the foundations for the Allies' later success at Bletchley Park."

Understanding what the cyclometer did

Rejewski's cyclometer exploited the German's procedure at the time of double encipherment of the Enigma message key, and semi-automated the process for calculating what were known as 'characteristics' for every possible Enigma rotor starting position. There were more than 100,000 of these rotor starting positions, and they each needed their characteristic to be calculated and catalogued in a card index system. The cyclometer therefore eliminated the arduous task of calculating these characteristics by hand.

The machine consisted of, in effect, two interlinked

Enigma systems side-by-side—one offset by three positions relative to the other—and 26 lamps and switches to cover the alphabet. On operation, a certain number of bulbs illuminated, indicating the lengths of the characteristics. These were recorded for every single possible rotor starting position to create an immense look-up catalogue. Once this was completed, obtaining the daily Enigma rotor starting settings to decode messages was a simple matter of intercepting enough messages and referencing the catalogue, taking only a matter of minutes.

Attempting this feat using a replica Enigma, which historians know were available to the Polish cryptographers, would have taken around 60 times longer than the nine months that it took with the aid of the cyclometer. This is what motivated Rejewski to design and build the cyclometer—the exploitation of cataloguing cycle lengths would not have been feasible in the timescales required without it.

Provided by University of Cambridge