Resurrecting the Bomba: Technical Abstract

Background

Before Alan Turing invented the Bombe, Polish cryptologist Marian Rejewski deciphered the German Enigma machines using another machine, termed the 'Bomba Kryptologiczna' or Cryptological Bomb. Before the German invasion of Poland, all the Bomby and details pertaining to them were destroyed.

Project Aims

This project aimed to recreate a working Bomba using equivalent technology, and to demonstrate the effectiveness of the Polish cryptological methods.

Enigma and the Bomba

An Enigma machine was an electromechanical rotor cipher machine used by Germany during the Second World War. Stepping wired rotors changed the cipher with every letter of the message, making it impossible to break using hand calculations. To increase the complexity of the machine, the Germans added a ring setting: a changeable offset between the rotor wiring and the rotor casing.

German Enigma operators would send an encoded key at the start of each message. Sometimes, a letter would be enciphered to the same thing twice. The Bomba exploited this operational flaw by parallel processing two Enigma machines to find the Enigma settings for which this double encoding could have occurred. To reduce the possible permutations of Enigma settings, three sets of parallel Enigmas were considered together.

A Bomba consisted of these six Enigma machines driven synchronously by a motor. A network of electrical relays identified each possible rotor configuration that could have caused the double encoding, and stopped the motor accordingly. The ring setting was then the difference between the rotor starting and stopping positions. This could be used on a replica Enigma machine to decrypt Enigma messages.

Bomba development

The project considered the mechanical and electrical aspects of the design as distinct subsystems.

The mechanical system was inspired by an odometer (milometer) as used to measure distance in a car. A central sun gear would turn each stack of Enigma rotors, and once per revolution an odometer would advance the next rotor in the stack in order to check all 17,576 possible rotor configurations.

The electrical subsystem used a network of transistors (as relays were too expensive), paired together. When the output of a parallel pair of Enigma machines was the same, the transistors would open and stop the motor.

Outcomes

The project had varying success: the electrical subsystems worked as intended, but the mechanical system was not able to reliably step the rotors. This was due to large friction forces between rotors, and also partially because the gear mechanism was made from MDF which found to be too weak to withstand the gear loads present in the system.

Next steps

Further work would look at developing a more robust drive mechanism, using data collected from the failed mechanism implemented in this project. It would also aim to characterise the behaviour of an Enigma machine using a software emulator developed as part of this project, so that the capabilities of the Bomba could be compared to those of its successor, the Turing Bombe.